

CVE-2019-14870	6.4	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	All Samba versions 4.x.x before 4.9.17, 4.10.x before 4.10.11 and 4.11.x before 4.11.3 have an issue, where the S4U (MS-SFU) Kerberos delegation model includes a feature allowing for a subset of clients to be opted out of constrained delegation in any way, either S4U2Self or regular Kerberos authentication, by forcing all tickets for these clients to be non-forwardable. In AD this is implemented by a user attribute delegation_not_allowed (aka not-delegated), which translates to disallow-forwardable. However the Samba AD DC does not do that for S4U2Self and does set the forwardable flag even if the impersonated client has the not-delegated flag set.
CVE-2019-14870	6.4	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	All Samba versions 4.x.x before 4.9.17, 4.10.x before 4.10.11 and 4.11.x before 4.11.3 have an issue, where the S4U (MS-SFU) Kerberos delegation model includes a feature allowing for a subset of clients to be opted out of constrained delegation in any way, either S4U2Self or regular Kerberos authentication, by forcing all tickets for these clients to be non-forwardable. In AD this is implemented by a user attribute delegation_not_allowed (aka not-delegated), which translates to disallow-forwardable. However the Samba AD DC does not do that for S4U2Self and does set the forwardable flag even if the impersonated client has the not-delegated flag set.
CVE-2017-12150	5.8	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	It was found that samba before 4.4.16, 4.5.x before 4.5.14, and 4.6.x before 4.6.8 did not enforce "SMB signing" when certain configuration options were enabled. A remote attacker could launch a man-in-the-middle attack and retrieve information in plain-text.
CVE-2017-12151	5.8	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in the way samba client before samba 4.4.16, samba 4.5.14 and samba 4.6.8 used encryption with the max protocol set as SMB3. The connection could lose the requirement for signing and encrypting to any DFS redirects, allowing an attacker to read or alter the contents of the connection via a man-in-the-middle attack.
CVE-2017-12150	5.8	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	It was found that samba before 4.4.16, 4.5.x before 4.5.14, and 4.6.x before 4.6.8 did not enforce "SMB signing" when certain configuration options were enabled. A remote attacker could launch a man-in-the-middle attack and retrieve information in plain-text.
CVE-2017-12151	5.8	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in the way samba client before samba 4.4.16, samba 4.5.14 and samba 4.6.8 used encryption with the max protocol set as SMB3. The connection could lose the requirement for signing and encrypting to any DFS redirects, allowing an attacker to read or alter the contents of the connection via a man-in-the-middle attack.
CVE-2019-14902	5.5	139	netbios- ssn	Samba smbd 4.6.2	2023-04-27 2023-05-06	There is an issue in all samba 4.11.x versions before 4.11.5, all samba 4.10.x versions before 4.10.12 and all samba 4.9.x versions before 4.9.18, where the removal of the right to create or modify a subtree would not automatically be taken away on all domain controllers.
CVE-2019-3880	5.5	139	netbios- ssn	Samba smbd 4.6.2	2023-04-27 2023-05-06	A flaw was found in the way samba implemented an RPC endpoint emulating the Windows registry service API. An unprivileged attacker could use this flaw to create a new registry hive file anywhere they have unix permissions which could lead to creation of a new file in the Samba share. Versions before 4.8.11, 4.9.6 and 4.10.2 are vulnerable.
CVE-2019-14902	5.5	445	netbios- ssn	Samba smbd 4.6.2	2023-04-27 2023-05-06	There is an issue in all samba 4.11.x versions before 4.11.5, all samba 4.10.x versions before 4.10.12 and all samba 4.9.x versions before 4.9.18, where the removal of the right to create or modify a subtree would not automatically be taken away on all domain controllers.
CVE-2019-3880	5.5	445	netbios- ssn	Samba smbd 4.6.2	2023-04-27 2023-05-06	A flaw was found in the way samba implemented an RPC endpoint emulating the Windows registry service API. An unprivileged attacker could use this flaw to create a new registry hive file anywhere they have unix permissions which could lead to creation of a new file in the Samba share. Versions before 4.8.11, 4.9.6 and 4.10.2 are vulnerable.
CVE-2017-15275	5.0	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	Samba before 4.7.3 might allow remote attackers to obtain sensitive information by leveraging failure of the server to clear allocated heap memory.
CVE-2020-10704	5.0	139		Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found when using samba as an Active Directory Domain Controller. Due to the way samba handles certain requests as an Active Directory Domain Controller LDAP server, an unauthorized user can cause a stack overflow leading to a denial of service. The highest threat from this vulnerability is to system availability. This issue affects all samba versions before 4.10.15, before 4.11.8 and before 4.12.2.
CVE-2020-27840	5.0	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in samba. Spaces used in a string around a domain name (DN), while supposed to be ignored, can cause invalid DN strings with spaces to instead write a zero-byte into out-of-bounds memory, resulting in a crash. The highest threat from this vulnerability is to system availability.
CVE-2021-20277	5.0	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in Samba's libldb. Multiple, consecutive leading spaces in an LDAP attribute can lead to an out-of- bounds memory write, leading to a crash of the LDAP server process handling the request. The highest threat from this vulnerability is to system availability.
CVE-2017-15275	5.0	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	Samba before 4.7.3 might allow remote attackers to obtain sensitive information by leveraging failure of the server to clear allocated heap memory.
CVE-2020-10704	5.0	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found when using samba as an Active Directory Domain Controller. Due to the way samba handles certain requests as an Active Directory Domain Controller LDAP server, an unauthorized user can cause a stack overflow leading to a denial of service. The highest threat from this vulnerability is to system availability. This issue affects all samba versions before 4.10.15, before 4.11.8 and before 4.12.2.
CVE-2020-27840	5.0	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in samba. Spaces used in a string around a domain name (DN), while supposed to be ignored, can cause invalid DN strings with spaces to instead write a zero-byte into out-of-bounds memory, resulting in a crash. The highest threat from this vulnerability is to system availability.
CVE-2021-20277	5.0	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in Samba's libldb. Multiple, consecutive leading spaces in an LDAP attribute can lead to an out-of- bounds memory write, leading to a crash of the LDAP server process handling the request. The highest threat from this vulnerability is to system availability.
CVE-2021-26712	5.0	5060	sip- proxy	Asterisk PBX 16.12.0	2023-04-27 2023-05-06	Incorrect access controls in res_srtp.c in Sangoma Asterisk 13.38.1, 16.16.0, 17.9.1, and 18.2.0 and Certified Asterisk 16.8-cert5 allow a remote unauthenticated attacker to prematurely terminate secure calls by replaying SRTP packets.
CVE-2021-26717	5.0	5060	sip- proxy	Asterisk PBX 16.12.0	2023-04-27 2023-05-06	An issue was discovered in Sangoma Asterisk 16.x before 16.16.1, 17.x before 17.9.2, and 18.x before 18.2.1 and Certified Asterisk before 16.8-cert6. When re-negotiating for T.38, if the initial remote response was delayed just enough, Asterisk would send both audio and T.38 in the SDP. If this happened, and the remote responded with a declined T.38 stream, then Asterisk would crash.
CVE-2021-32558	5.0	5060	sip- proxy	Asterisk PBX 16.12.0	2023-04-27 2023-05-06	An issue was discovered in Sangoma Asterisk 13.x before 13.38.3, 16.x before 16.19.1, 17.x before 17.9.4, and 18.x before 18.5.1, and Certified Asterisk before 16.8-cert10. If the IAX2 channel driver receives a packet that contains an unsupported media format, a crash can occur.
CVE-2019-14833	4.9	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in Samba, all versions starting samba 4.5.0 before samba 4.9.15, samba 4.10.10, samba 4.11.2, in the way it handles a user password change or a new password for a samba user. The Samba Active Directory Domain Controller can be configured to use a custom script to check for password complexity. This configuration can fail to verify password complexity when non-ASCII characters are used in the password, which could lead to weak passwords being set for samba users, making it vulnerable to dictionary attacks.
CVE-2021-20254	4.9	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in samba. The Samba smbd file server must map Windows group identities (SIDs) into unix group ids (gids). The code that performs this had a flaw that could allow it to read data beyond the end of the array in the case where a negative cache entry had been added to the mapping cache. This could cause the calling code to return those values into the process token that stores the group membership for a user. The highest threat from this vulnerability is to data confidentiality and integrity.
CVE-2019-14833	4.9	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	valuerability is to data confidentiality and integrity.  A flaw was found in Samba, all versions starting samba 4.5.0 before samba 4.9.15, samba 4.10.10, samba 4.11.2, in the way it handles a user password change or a new password for a samba user. The Samba Active Directory Domain Controller can be configured to use a custom script to check for password complexity. This configuration can fail to verify password complexity when non-ASCII characters are used in the password, which could lead to weak passwords being set for samba users, making it vulnerable to dictionary attacks.
CVE-2021-20254	4.9	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in samba. The Samba smbd file server must map Windows group identities (SIDs) into unix group ids (gids). The code that performs this had a flaw that could allow it to read data beyond the end of the array in the case where a negative cache entry had been added to the mapping cache. This could cause the calling code to return those values into the process token that stores the group membership for a user. The highest threat from this vulnerability is to data confidentiality and integrity.
CVE-2017-12163	4.8	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	An information leak flaw was found in the way SMB1 protocol was implemented by Samba before 4.4.16, 4.5.x before 4.5.14, and 4.6.x before 4.6.8. A malicious client could use this flaw to dump server memory contents to a file on the samba share or to a shared printer, though the exact area of server memory cannot be controlled by the attacker.
CVE-2017-12163	4.8	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	An information leak flaw was found in the way SMB1 protocol was implemented by Samba before 4.4.16, 4.5.x before 4.5.14, and 4.6.x before 4.6.8. A malicious client could use this flaw to dump server memory contents to a file on the samba share or to a shared printer, though the exact area of server memory cannot be controlled by the attacker.

CVE-2016-2124	4.3	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in the way samba implemented SMB1 authentication. An attacker could use this flaw to retrieve the plaintext password sent over the wire even if Kerberos authentication was required.
CVE-2016-2124	4.3	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in the way samba implemented SMB1 authentication. An attacker could use this flaw to retrieve the plaintext password sent over the wire even if Kerberos authentication was required.
CVE-2020-35776	4.3	5060		Asterisk PBX 16.12.0	2023-04-27 2023-05-06	A buffer overflow in res_pjsip_diversion.c in Sangoma Asterisk versions 13.38.1, 16.15.1, 17.9.1, and 18.1.1 allows remote attacker to crash Asterisk by deliberately misusing SIP 181 responses.
CVE-2021-26906	4.3	5060		Asterisk PBX 16.12.0	2023-04-27 2023-05-06	An issue was discovered in res_pjsip_session.c in Digium Asterisk through 13.38.1; 14.x, 15.x, and 16.x through 16.16.0; 17.x through 17.9.1; and 18.x through 18.2.0, and Certified Asterisk through 16.8-cert5. An SDP negotiation vulnerability in PJSIP allows a remote server to potentially crash Asterisk by sending specific SIP responses that cause an SDP negotiation failure.
CVE-2018-10919	4.0	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	The Samba Active Directory LDAP server was vulnerable to an information disclosure flaw because of missing access control checks. An authenticated attacker could use this flaw to extract confidential attribute values using LDAP search expressions. Samba versions before 4.6.16, 4.7.9 and 4.8.4 are vulnerable.
CVE-2018-14629	4.0	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A denial of service vulnerability was discovered in Samba's LDAP server before versions 4.7.12, 4.8.7, and 4.9.3. A CNAME loop could lead to infinite recursion in the server. An unprivileged local attacker could create such an entry, leading to denial of service.
CVE-2018-16841	4.0	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	Samba from version 4.3.0 and before versions 4.7.12, 4.8.7 and 4.9.3 are vulnerable to a denial of service. When configured to accept smart-card authentication, Samba's KDC will call talloc_free() twice on the same memory if the principal in a validly signed certificate does not match the principal to the AS-REQ. This is only possible after authentication with a trusted certificate. talloc is robust against further corruption from a double-free with talloc_free() and directly calls abort(), terminating the KDC process.
CVE-2018-16851	4.0	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	Samba from version 4.0.0 and before versions 4.7.12, 4.8.7, 4.9.3 is vulnerable to a denial of service. During the processing of an LDAP search before Samba's AD DC returns the LDAP entries to the client, the entries are cached in a single memory object with a maximum size of 256MB. When this size is reached, the Samba process providing the LDAP service will follow the NULL pointer, terminating the process. There is no further vulnerability associated with this issue, merely a denial of service.
CVE-2019-14847	4.0	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in samba 4.0.0 before samba 4.9.15 and samba 4.10.x before 4.10.10. An attacker can crash AD DC LDAP server via dirsync resulting in denial of service. Privilege escalation is not possible with this issue.
CVE-2020-10730	4.0	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A NULL pointer dereference, or possible use-after-free flaw was found in Samba AD LDAP server in versions before 4.10.17, before 4.11.11 and before 4.12.4. Although some versions of Samba shipped with Red Hat Enterprise Linux do not support Samba in AD mode, the affected code is shipped with the libldb package. This flaw allows an authenticated user to possibly trigger a use-after-free or NULL pointer dereference. The highest threat from this vulnerability is to system availability.
CVE-2020-10760	4.0	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A use-after-free flaw was found in all samba LDAP server versions before 4.10.17, before 4.11.11, before 4.12.4 used in a AC DC configuration. A Samba LDAP user could use this flaw to crash samba.
CVE-2020-14318	4.0	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in the way samba handled file and directory permissions. An authenticated user could use this flaw to gain access to certain file and directory information which otherwise would be unavailable to the attacker.
CVE-2020-14383	4.0	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in samba's DNS server. An authenticated user could use this flaw to the RPC server to crash. This RPC server, which also serves protocols other than dnsserver, will be restarted after a short delay, but it is easy for an authenticated non administrative attacker to crash it again as soon as it returns. The Samba DNS server itself will continue to operate, but many RPC services will not.
CVE-2018-10919	4.0	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	The Samba Active Directory LDAP server was vulnerable to an information disclosure flaw because of missing access control checks. An authenticated attacker could use this flaw to extract confidential attribute values using LDAP search expressions. Samba versions before 4.6.16, 4.7.9 and 4.8.4 are vulnerable.
CVE-2018-14629	4.0	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A denial of service vulnerability was discovered in Samba's LDAP server before versions 4.7.12, 4.8.7, and 4.9.3. A CNAME loop could lead to infinite recursion in the server. An unprivileged local attacker could create such an entry, leading to denial of service.
CVE-2018-16841	4.0	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	Samba from version 4.3.0 and before versions 4.7.12, 4.8.7 and 4.9.3 are vulnerable to a denial of service. When configured to accept smart-card authentication, Samba's KDC will call talloc_free() twice on the same memory if the principal in a validly signed certificate does not match the principal in the AS-REQ. This is only possible after authentication with a trusted certificate. talloc is robust against further corruption from a double-free with talloc_free() and directly calls abort(), terminating the KDC process.
CVE-2018-16851	4.0	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	Samba from version 4.0.0 and before versions 4.7.12, 4.8.7, 4.9.3 is vulnerable to a denial of service. During the processing of an LDAP search before Samba's AD DC returns the LDAP entries to the client, the entries are cached in a single memory object with a maximum size of 256MB. When this size is reached, the Samba process providing the LDAP service will follow the NULL pointer, terminating the process. There is no further vulnerability associated with this issue, merely a denial of service.
CVE-2019-14847	4.0	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in samba 4.0.0 before samba 4.9.15 and samba 4.10.x before 4.10.10. An attacker can crash AD DC LDAP server via dirsync resulting in denial of service. Privilege escalation is not possible with this issue.
CVE-2020-10730	4.0	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A NULL pointer dereference, or possible use-after-free flaw was found in Samba AD LDAP server in versions before 4.10.17, before 4.11.11 and before 4.12.4. Although some versions of Samba shipped with Red Hat Enterprise Linux do not support Samba in AD mode, the affected code is shipped with the libldb package. This flaw allows an authenticated user to possibly trigger a use-after-free or NULL pointer dereference. The highest threat from this vulnerability is to system availability.
CVE-2020-10760	4.0	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A use-after-free flaw was found in all samba LDAP server versions before 4.10.17, before 4.11.11, before 4.12.4 used in a AC DC configuration. A Samba LDAP user could use this flaw to crash samba.
CVE-2020-14318	4.0	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in the way samba handled file and directory permissions. An authenticated user could use this flaw to gain access to certain file and directory information which otherwise would be unavailable to the attacker.
CVE-2020-14383	4.0	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in samba's DNS server. An authenticated user could use this flaw to the RPC server to crash. This RPC server, which also serves protocols other than dnsserver, will be restarted after a short delay, but it is easy for an authenticated non administrative attacker to crash it again as soon as it returns. The Samba DNS server itself will continue to operate, but many RPC services will not.
CVE-2020-35652  General Security Is:	4.0	5060	sip- proxy	Asterisk PBX 16.12.0	2023-04-27 2023-05-06	An issue was discovered in res_pjsip_diversion.c in Sangoma Asterisk before 13.38.0, 14.x through 16.x before 16.15.0, 17.x before 17.9.0, and 18.x before 18.1.0. A crash can occur when a SIP message is received with a History-Info header that contains a tel-uri, or when a SIP 181 response is received that contains a tel-uri in the Diversion header.
CVE Severity De		ion				Port Service Service Version First Seen Last Seen Remediation Reference
				nd/or other sensitiv	e data sent plaintext	21 ftp vsftpd 3.0.5 2022-03-02 2023-04-19 disable FTP and migrate to secure STFP or
(w	ithout (	encryp	otion)			SCP protocol

Showing 1 results.
Showing 76 results.
Note: Low-ranked results are informational-only or otherwise inactionable and are thus excluded from this listing.

ostname	proxmo	x					
perating Syste	•						
S Version							
PE							
IC Vendor							
rst Seen	2023-04	1-27					
ast Seen	2023-05	5-06					
ritical CVSS							
IGH CVSS							
EDIUM CVSS	4						
OW CVSS	1						
VSS Total	5						
orts							
	Protocol	Service	Service Version		CPE Has	Exploits? Verified Service Verified Version First Se	een Last Se
22	tcp	ssh	OpenSSH 8.4p1 Deb	nian 5+deb11u1 (protocol 2.0	cpe:/a:openbsd:openssh:8.4p1:	2023-0-	4-27 2023-05
111	tcp	rpcbind	2-4 (RPC #100000)			2023-0-	4-27 2023-05
3128	tcp	http	Proxmox Virtual Envi	ronment REST API 3.0		2023-0-	4-27 2023-05
8006	tcp	wpl-analytics	;?			2023-04	4-27 2023-05
Showing	•	1					
/E Scores CVE	CVSS	Port Servic	e Service Version	First Seen Last Seen	Description		
CVE-2021-280			OpenSSH 8.4p1		•	a double free that may be relevant in a few less-common	n econorios
CVL-2021-200	741 4.0	22 3311	Debian 5+deb11u1 (protocol 2.0)			ccess on a legacy operating system, or the forwarding of	
CVE-2021-416	617 4.4	22 ssh	OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)		escalation because supplemental group AuthorizedKeysCommand and Authoriz	re 8.8, when certain non-default configurations are used ps are not initialized as expected. Helper programs for zedPrincipalsCommand may run with privileges associat e configuration specifies running the command as a diffe	ted with group
CVE-2016-200	012 4.3	22 ssh	OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)		combination of username and public ke This occurs because a challenge is sen	allows remote attackers, who have a suspicion that a co by is known to an SSH server, to test whether this suspic nt only when that combination could be valid for a login s umeration as a vulnerability for this product.	ion is correct.
			OpenSSH 8.4p1	2022 04 27 2022 05 00	The client side in OpenSSH 5.7 through	h 8.4 has an Observable Discrepancy leading to an infor	mation leak ir

### 192.168.2.84 Hostname ciscophone.bibleheroes Operating System OS Version CPE NIC Vendor (Cisco Systems) First Seen 2022-02-27 2023-05-06 Last Seen Critical CVSS HIGH CVSS MEDIUM CVSS LOW CVSS CVSS Total CPE Has Exploits? Verified Service Verified Version Number Protocol Service Service Version First Seen Last Seen 68 udp dhcpc 80 tcp http Cisco SPA504G http config 5060 udp sip 2023-04-27 2023-05-06 2022-02-27 2023-05-06 2023-04-27 2023-05-06 54321 udp bo2k 2023-04-27 2023-05-06 Showing 4 results.

JZ.100	3.2.88											
ostname	е	freekde										
perating		FreeBS	D									
S Versioi												
PE		cpe:/o:f	reebsd:f	reebso	d							
 IC Vendo	or				tual NIC)							
rst Seen		2022-0		OX VIII	iddi Woj							
ast Seen		2023-0										
ritical CV		2023-0	3-00									
IGH CVS												
		7										
EDIUM C		7 7										
VSS Tota	aı	14										
orts												
	lumber I	Protoco	I Servic	e Se	ervice Version			CPE I	Has Exploits?	Verified Service	Verified Version	First Seen Last S
22	2 t	tcp	ssh	O	penSSH 8.8 (FreeBSD	20211221: protoc	col 2 (1)	cpe:/a:openbsd:openssh:8.8:	•			2022-02-27 2023-
25		tcp	smtp		ostfix smtnd	LOLLILLI, protoc	JO. 2.0)	орожи орожи орожиот положи.				2022-02-27 2023-
						- DCD) DUD/7 4 4	20)					
80		tcp	http		pache httpd 2.4.55 ((Fre	ee650) PHP/7.4.3	32)	cpe:/a:apache:http_server:2.4.55:				2022-02-27 2023-
35	57 t	tcp	bheve	nt								2022-02-27 2023-
44	43 t	tcp	https									2022-02-27 2023-
59	901 t	tcp	vnc	1V	NC (protocol 3.8)							2022-02-27 2023-
94	465 t	tcp	unknov	νn								2022-02-27 2023-
QF	587 t	tcp	unknov	۸'n								2022-02-27 2023-
		tcp	palace									2022-02-27 2023-
		•	•									
99		tcp	palace	-4								2022-02-27 2023-
E Score	ŭ	0 results		ervice	Service Version	First Seen Las	st Seen	Description				
E Score	es	cvss	Port Se		Service Version Apache httpd 2.4.55	First Seen Las 2022-02-27 202		·	ı cause a buffer	overflow in the m	od lua multipart pa	
E Score CVE CVE-202 Exclusion NOTIMPL	es 021-44790 on Reason: LEMENTED	CVSS	Port Se	tp	Apache httpd 2.4.55 ((FreeBSD) PHP/7.4.32)	2022-02-27 202	22-03-04	A carefully crafted request body can from Lua scripts). The Apache httpd to craft one. This issue affects Apach	team is not awa he HTTP Serve	are of an exploit f r 2.4.51 and earli	or the vulnerabilty ther.	rser (r:parsebody() c nough it might be po
E Score CVE CVE-202 Exclusion NOTIMPL	es 021-44790 on Reason:	CVSS	Port Se	tp	Apache httpd 2.4.55 ((FreeBSD) PHP/7.4.32)	2022-02-27 202	22-03-04	A carefully crafted request body can from Lua scripts). The Apache httpd	team is not awa he HTTP Serve ed as a forward nixing forward an Socket endpoin	are of an exploit f r 2.4.51 and earli proxy (ProxyReq nd reverse proxy	or the vulnerabilty ther. er. uests on) can cause declarations, can al	rser (r:parsebody() c nough it might be po e a crash (NULL poir low for requests to b
E Score CVE-202 Exclusion NOTIMPL CVE-202	21-4479( on Reason: LEMENTED 021-44224	CVSS 0 7.5 4 6.4	Port Se	tp tp	Apache httpd 2.4.55 ((FreeBSD) PHP/7.4.32) Apache httpd 2.4.55 ((FreeBSD)	2022-02-27 202	22-03-04 22-03-04	A carefully crafted request body can from Lua scripts). The Apache httpd to craft one. This issue affects Apach A crafted URI sent to httpd configure dereference) or, for configurations m directed to a declared Unix Domain HTTP Server 2.4.7 up to 2.4.51 (incl An issue was discovered in OpenSS chooses which files/directories are s the object name returned (only direc Middle attacker) can overwrite arbitr performed, the server can manipulat	team is not awa he HTTP Server ed as a forward nixing forward an Socket endpoin luded). SH 7.9. Due to the sent to the client ctory traversal at tary files in the s	are of an exploit f 2.4.51 and earli proxy (ProxyReq dd reverse proxy t (Server Side Re le scp implement However, the sc tacks are preven cp client target di	or the vulnerability ther.  uests on) can cause declarations, can al quest Forgery). Thi ation being derived p client only perfor ted). A malicious sorectory, if recursive	rser (r:parsebody() o nough it might be po e a crash (NULL poir low for requests to b is issue affects Apac from 1983 rcp, the s ins cursory validatior p server (or Man-in- operation (-r) is
E Score CVE CVE-202 Exclusion NOTIMPL CVE-202 CVE-202	es	CVSS 7.5 4 6.4 5.8	Port So 80 ht 80 ht 22 ss	tp tp sh	Apache httpd 2.4.55 ((FreeBSD) PHP/7.4.32) Apache httpd 2.4.55 ((FreeBSD) PHP/7.4.32) OpenSSH 8.8 (FreeBSD 20211221; protocol 2.0)	2022-02-27 202 2022-02-27 202 2022-02-27 202	22-03-04 22-03-04 22-03-14	A carefully crafted request body can from Lua scripts). The Apache httpd to craft one. This issue affects Apacl A crafted URI sent to httpd configure dereference) or, for configurations m directed to a declared Unix Domain HTTP Server 2.4.7 up to 2.4.51 (incl An issue was discovered in OpenSS chooses which files/directories are s the object name returned (only direc Middle attacker) can overwrite arbitra performed, the server can manipulat file).	team is not awa he HTTP Serve ed as a forward nixing forward at Socket endpoin luded). SH 7.9. Due to the sent to the client ctory traversal at tary files in the s te subdirectories	are of an exploit for 2.4.51 and earli r 2.4.51 and earli proxy (ProxyReq do reverse proxy t (Server Side Re ne scp implement However, the sc tacks are preven cp client target dis as as well (for example)	or the vulnerability it ex. usests on) can cause declarations, can al quest Forgery). Thi ation being derived p client only perfor ted). A malicious so rectory. If recursive mple, to overwrite th	rser (r:parsebody() on ough it might be potentially a crash (NULL poin low for requests to be sissue affects Apac from 1983 rcp, the sins cursory validation pierver (or Man-in-operation (-r) is the instance of the control of the co
E Score CVE CVE-202 Exclusion NOTIMPL CVE-202 CVE-202	21-4479( on Reason: LEMENTED 021-44224	CVSS 7.5 4 6.4 5.8	Port So 80 ht 80 ht 22 ss	tp tp sh	Apache httpd 2.4.55 ((FreeBSD) PHP/T.4.32) Apache httpd 2.4.55 ((FreeBSD) PHP/T.4.32) OpenSSH 8.8 (FreeBSD 20211221;	2022-02-27 202 2022-02-27 202 2022-02-27 202	22-03-04 22-03-04 22-03-14	A carefully crafted request body can from Lua scripts). The Apache httpd to craft one. This issue affects Apach A crafted URI sent to httpd configure dereference) or, for configurations m directed to a declared Unix Domain HTTP Server 2.4.7 up to 2.4.51 (incl An issue was discovered in OpenSS chooses which files/directories are s the object name returned (only direc Middle attacker) can overwrite arbitr performed, the server can manipulat	I team is not aware HTTP Serve- ed as a forward an Socket endpoin luded).  Sh T.9. Due to the service of the client to the client to the client to the service of an elimental in all relimental in all reliments.	are of an exploit for 2.4.51 and earli 2.4.51 and earli proxy (ProxyReq dr everse proxy t (Server Side Re ene scp implement However, the sc tacks are preven cp client target di s as well (for exal compiled with an compiled with ar configured to us error in the XMSS	or the vulnerability it ex- usests on) can cause declarations, can al quest Forgery). Thi ation being derived p client only perforted). A malicious so rectory. If recursive mple, to overwrite it experimental key to a crafted XMSS k key parsing algorit	rser (r:parsebody() onough it might be po e a crash (NULL poin low for requests to b is issue affects Apac from 1983 rcp, the s ins cursory validation p server (or Man-in- operation (-r) is ie .ssh/authorized_k ype, has a pre- ey. This leads to me hm. NOTE: the XMS
E Score CVE CVE-202 Exclusion NOTIMPL CVE-202 CVE-202	es	CVSS 7.5 4 6.4 5.8 5 4.4	Port So 80 ht 80 ht 22 ss	ttp ttp sh	Apache httpd 2.4.55 ((FreeBSD) PHP/7.4.32) Apache httpd 2.4.55 ((FreeBSD) PHP/7.4.32) OpenSSH 8.8 (FreeBSD 20211221; protocol 2.0) OpenSSH 8.8 (FreeBSD 20211221;	2022-02-27 202 2022-02-27 202 2022-02-27 202 2022-02-27 202	22-03-04 22-03-14 22-03-14	A carefully crafted request body can from Lua scripts). The Apache httpd to craft one. This issue affects Apacl A crafted URI sent to httpd configure dereference) or, for configurations m directed to a declared Unix Domain : HTTP Server 2.4.7 up to 2.4.51 (incl. An issue was discovered in OpenSS chooses which files/directories are s the object name returned (only direc Middle attacker) can overwrite arbitra performed, the server can manipulat file).  OpenSSH 7.7 through 7.9 and 8.x bis authentication integer overflow if a circorruption and local code execution implementation is considered experi	I team is not awith the HTTP Serve and as a forward and socket endpoin luded). SH 7.9. Due to the service and	are of an exploit fr 2.4.51 and earli 7.2.4.51 and earli proxy (ProxyReq dr everse proxy tr (Server Side Re ne scp implement. However, the sc tacks are preven collent target di s as well (for exai compiled with are configured to us error in the XMSS eased OpenSSH certain non-defat tailized as expect Command may r	or the vulnerability tiger.  uests on) can cause declarations, can al quest Forgery). Thi ation being derived p client only performed). A malicious screetory. If recursive mple, to overwrite the experimental key te a crafted XMSS k key parsing algorit versions, and there ult configurations ared. Helper program un with privileges a	rser (r:parsebody() or nough it might be po e a crash (NULL poir low for requests to b is issue affects Apac from 1983 rcp, the sins cursory validation p server (or Man-in-operation (-r) is in e.ssh/authorized_k ype, has a pre-ey. This leads to me him. NOTE: the XMS is no supported way e used, allows privile is for ssociated with group special processories.
E Score CVE CVE-202 Exclusion NOTIMPL CVE-202 CVE-202 CVE-202 CVE-202	021-4479( pon Reason: LEMENTED 021-4422( 019-6111	CVSS 0 7.5 4 6.4 5.8 5 4.4 7 4.4	Port So 80 ht 80 ht 22 ss	tp tp sh	Apache httpd 2.4.55 ((FreeBSD) PHP/7.4.32) Apache httpd 2.4.55 ((FreeBSD) PHP/7.4.32)  OpenSSH 8.8 (FreeBSD 20211221; protocol 2.0)  OpenSSH 8.8 (FreeBSD 20211221; protocol 2.0)  OpenSSH 8.8 (FreeBSD 20211221;	2022-02-27 202 2022-02-27 202 2022-02-27 202 2022-02-27 202 2022-02-27 202	22-03-04 22-03-04 22-03-14 22-03-14	A carefully crafted request body can from Lua scripts). The Apache httpd to craft one. This issue affects Apacl A crafted URI sent to httpd configure dereference) or, for configurations m directed to a declared Unix Domain : HTTP Server 2.4.7 up to 2.4.51 (incl An issue was discovered in OpenSS chooses which files/directories are s the object name returned (only direc Middle attacker) can overwrite arbitric performed, the server can manipulat file).  1 OpenSSH 7.7 through 7.9 and 8.x be authentication integer overflow if a ci corruption and local code execution implementation is considered experienable it when building portable Opes sshd in OpenSSH 6.2 through 8.x be escalation because supplemental graduthorizedKeysCommand and AuthorizedKeysCommand and Authorize	I team is not aw. he HTTP Serve as a sa forward nixing forward at Socket endpoin luded).  SH 7.9. Due to the sent to the client to the client ctory traversal at any files in the stee subdirectories the subdirectories are subdirectories. The second is a subdirectories are subdirectories are subdirectories and the subdirectories are subdirectories. The subdirectories are not subdirectories are subdirectories are not iniorized Principals the configuration upgh 8.4 has an an-in-the-middle.	are of an exploit for 2.4.51 and earli 7.2.4.51 and earli proxy (ProxyReq dr everse proxy t (Server Side Research en esp implement. However, the sc tacks are preven compiled with an configured to use error in the XMSS error in the XMSS error in the XMSS compiled with an configured to use error in the XMSS error in the	or the vulnerability ties event to the vulnerability to event to the vulnerability ation being derived p client only perform ted). A malicious so rectory. If recursive mple, to overwrite the e a crafted XMSS ke e a crafted XMSS ke key parsing algority versions, and there ult configurations are ted. Helper program un with privileges a ng the command as epeancy leading to a let initial connection eater initial connection experience.	rser (r:parsebody() or nough it might be po et a crash (NULL poir low for requests to be sissue affects Apac from 1983 rcp, the sins cursory validation p server (or Man-in-operation (-r) is le. s.sh/authorized_k ype, has a preey. This leads to me hm. NOTE: the XMS is no supported way et used, allows privile is for ssociated with group a different user. In information leak ir attempts (where no ino inour mation leak ir attempts (where no inour information leak ir attempts (where no inour inour information leak ir attempts (where no inour
CVE-202 CVE-202 CVE-202 CVE-202 CVE-202 CVE-202	021-4479000 Reason: LEMENTED 021-44220 0019-6111 0019-16900	CVSS 0 7.5 6.4 6.4 6.4 6.4 7 7 4.4 5 5 4.3	Port Sc 80 ht 80 ht 22 ss 22 ss 22 ss	tp tp sh	Apache httpd 2.4.55 ((FreeBSD) PHP/7.4.32) Apache httpd 2.4.55 ((FreeBSD) PHP/7.4.32) OpenSSH 8.8 (FreeBSD 20211221; protocol 2.0)	2022-02-27 202 2022-02-27 202 2022-02-27 202 2022-02-27 202 2022-02-27 202	22-03-04 22-03-04 22-03-14 22-03-14 23-05-06	A carefully crafted request body can from Lua scripts). The Apache httpd to craft one. This issue affects Apacl A crafted URI sent to httpd configure dereference) or, for configurations m directed to a declared Unix Domain : HTTP Server 2.4.7 up to 2.4.51 (incl. An issue was discovered in OpenSS chooses which files/directories are s the object name returned (only direc Middle attacker) can overwrite arbitra performed, the server can manipulat file).  OpenSSH 7.7 through 7.9 and 8.x be authentication integer overflow if a ci corruption and local code execution implementation is considered experienable it when building portable Ope sshd in OpenSSH 6.2 through 8.x be escalation because supplemental gn AuthorizedKeysCommand and Authenemberships of the sshd process, if The client side in OpenSSH 5.7 through growth allows me.	I team is not awin the HTTP Serve and as a forward an Socket endpoin luded).  SH 7.9. Due to the tent to the client to the client tory traversal at any files in the set to subdirectories the subdirectories are files in the set to subdirectories are files in the set to subdirectories are files in the set to subdirectories are files and in all relient or server is because of an elimental in all relients should be subdirectories. SH.  Lefore 8.8, when roups are not initial orized principals to the configuration of the configuration of the configuration of the set of th	are of an exploit for 2.4.51 and earli 2.4.51 and earli proxy (ProxyReq and reverse proxy to (Server Side Reverse Side Rev	or the vulnerability the car.  usests on) can cause declarations, can all quest Forgery). Thi ation being derived p client only performed). A malicious screetory. If recursive mple, to overwrite the each acrafted XMSS is experimental key the each acrafted the configurations are the configurations	rser (r:parsebody() or nough it might be po e a crash (NULL poir low for requests to b is issue affects Apac from 1983 rcp, the s ns cursory validation peration (-r) is e. ssh/authorized_k ype, has a pre-ey. This leads to me hm. NOTE: the XMS is no supported way e used, allows privile is for ssociated with group a different user. In information leak in attempts (where no 8 8.6 are also affecte gress display, a mall he client output, e.g.

**Note:** Low-ranked results are informational-only or otherwise inactionable and are thus excluded from this listing

# 192.168.2.112

Hostname Operating System
OS Version

CPE

NIC Vendor First Seen

2023-04-27 Last Seen 2023-05-06

Critical CVSS HIGH CVSS MEDIUM CVSS LOW CVSS CVSS Total

# Ports

Number	Protocol	Service	Service Version	CPE H	las Exploits?	Verified Service	Verified Version	First Seen	Last Seen
135	tcp	msrpc	Microsoft Windows RPC					2023-04-27	2023-04-27
137	udp	netbios-ns	Microsoft Windows netbios-ns (workgroup: WORKGROUP)					2023-04-27	2023-04-27
139	tcp	netbios-ssn	Microsoft Windows netbios-ssn					2023-04-27	2023-04-27
445	tcp	microsoft-ds?						2023-04-27	2023-04-27
5040	tcp	unknown						2023-04-27	2023-04-27
5357	tcp	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)					2023-04-27	2023-04-27
5693	tcp	ssl/http	Ajenti http control panel					2023-04-27	2023-04-27
7680	tcp	pando-pub?						2023-04-27	2023-04-27
49668	tcp	msrpc	Microsoft Windows RPC					2023-04-27	2023-04-27
Showing	9 results.								

5/18/23, 08:54 8 of 27

### 192.168.2.113 Hostname freebsd131pve Operating System FreeBSD OS Version cpe:/o:freebsd:freebsd CPE NIC Vendor First Seen 2023-04-27 2023-05-06 Last Seen Critical CVSS HIGH CVSS MEDIUM CVSS 1 LOW CVSS 1 CVSS Total Ports CPE Number Protocol Service Service Version Has Exploits? Verified Service Verified Version First Seen Last Seen 22 tcp ssh OpenSSH 8.8 (FreeBSD 20211221; protocol 2.0) cpe:/a:openbsd:openssh:8.8: 2023-04-27 2023-05-06 Showing 1 results. CVE Scores CVSS Port Service Service Version First Seen Last Seen Description CVE CVE-2021-41617 4.4 22 sh OpenSSH 8.8 (FreeBSD 20211221; protocol 2.0) OpenSSH 8.8 AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privilege associated with group memberships of the sshd process, if the configuration specifies running the command as a different user. Showing 1 results. Note: Low-ranked results are informational-only or otherwise inactionable and are thus excluded from this listing.

### 192.168.2.114 Hostname slack15pve Operating System OS Version CPE NIC Vendor First Seen 2023-04-26 2023-05-06 Last Seen Critical CVSS HIGH CVSS MEDIUM CVSS LOW CVSS CVSS Total Verified Verified Number Protocol Service Service Version CPE Has First Seen Last Seen Exploits? Service Version 22 tcp ssh OpenSSH 9.3 (protocol 2.0) 2023-04-27 2023-05-06 25 tcp smtp Postfix smtpd 80 tcp http Apache httpd 2.4.57 ((Unix) mod\_apreq2-20101207/2.8.1 mod\_perl/2.0.12 Perl/v5.34.0) 2023-04-27 2023-05-06 2023-04-27 2023-05-06 161 udp snmp net-snmp; net-snmp SNMPv3 server Showing 4 results. 2023-04-27 2023-05-06

stname									
		chin							
erating Sys	stem								
Version									
E									
C Vendor	(Inte	l Corporate	)						
st Seen	2022	2-02-27							
st Seen	2023	3-05-06							
tical CVSS									
SH CVSS									
DIUM CVS	<b>S</b> 10								
W CVSS	6								
SS Total	16								
33 Iolai	10								
ts									
Numbe	er Protoco	ol Service	Service Version		CPE	Has Exploits?	Verified Service	Verified Version	First Seen Last Se
37	tcp	time	(32 bits)						2022-02-27 2023-05
53	tcp	domain	(unknown banner: Apache 1.3)						2022-02-27 2023-05
80	tcp	http	Apache httpd 2.4.55 ((Unix) mod_ap	reg2-20090110/2 8 0	cpe:/a:apache:http_server:2.4.55:				2022-02-27 2023-05
80	ıср	пцр	mod perl/2.0.11 Perl/v5.22.2)	11642-20030110/2.0.0	cpe./a.apacne.nup_server.2.4.55				2022-02-21 2023-05
113	tcp	ident							2022-02-27 2023-0
123	udp	ntp?							2023-04-27 2023-0
139	tcp	netbios- ssn	Samba smbd 3.X - 4.X (workgroup:	BIBLEHEROES)					2022-02-27 2023-0
357	tcp	ssh	OpenSSH 7.4 (protocol 2.0)		cpe:/a:openbsd:openssh:7.4:	Yes			2022-02-27 2023-05
445	tcp	netbios- ssn	Samba smbd 3.X - 4.X (workgroup:	BIBLEHEROES)					2022-02-27 2023-05
1714	tcp	sesi-lm?							2022-02-27 2023-0
Snowing	g 9 results	i.							
E Scores									
CVE	CV:	SS Port S	ervice Service Version	First Seen Last See	n Description				
CVE-2021-4 Exclusion Rea		5 80 ht	tp Apache httpd 2.4.55 ((Unix) mod_apreq2-20090110/2.8.0	2022-02-27 2022-03-	14 A carefully crafted request body (r:parsebody() called from Lua s				
CVE-2021-4	son:	5 80 ht		2022-02-27 2022-03-	(r:parsebody() called from Lua s vulnerabilty though it might be p	scripts). The A	pache httpd	team is not aw	are of an exploit for the
Exclusion Rea.	son: VTED		mod_apreq2-20090110/2.8.0 mod_perl/2.0.11 Perl/v5.22.2)		(r:parsebody() called from Lua s vulnerabilty though it might be p and earlier.	scripts). The A possible to craf	pache httpd t one. This i	team is not aw ssue affects Ap	are of an exploit for the pache HTTP Server 2.4.
Exclusion Rea.	son: VTED	80 ht	mod_apreq2-20090110/2.8.0 mod_perl/2.0.11 Perl/v5.22.2)		(r:parsebody() called from Lua s vulnerabilty though it might be p	scripts). The A possible to craf figured as a for for configuration ected to a declar	pache httpd it one. This is ward proxy ons mixing fo ared Unix Do	team is not aw ssue affects Ap (ProxyRequest orward and rev omain Socket e	are of an exploit for the bache HTTP Server 2.4. Its on) can cause a crast erse proxy declarations, endpoint (Server Side
EVE-2021-4 Exclusion Rea: NOTIMPLEMEN	son: NTED 4224 6		mod_apreq2-20090110/2.8.0 mod_perl/2.0.11 Perl/v5.22.2) tp Apache httpd 2.4.55 ((Unix) mod_apreq2-20090110/2.8.0 mod_perl/2.0.11 Perl/v5.22.2)	2022-02-27 2022-03-	(r:parsebody() called from Lua sulnerability though it might be pand earlier.  14 A crafted URI sent to httpd cont (NULL pointer dereference) or, can allow for requests to be dire Request Forgery). This issue at 06 An issue was discovered in Opprop, the server chooses which finerforms cursory validation of the prevented). A malicious scp ser the scp client target directory.	scripts). The Apossible to craffigured as a for for configuratic ected to a declifects Apache I enSSH 7.9. Dulles/directories he object name ver (or Man-in recursive oper	ward proxy ons mixing for ared Unix Do HTTP Serve te to the scp are sent to the returned (o The-Middle ration (-r) is	team is not awassue affects Ap (ProxyRequesi oward and rev omain Socket of 2.4.7 up to 2. implementatio the client. How nily directory tr attacker) can a performed, the	are of an exploit for the bache HTTP Server 2.4 its on) can cause a cras erse proxy declarations endpoint (Server Side 4.51 (included). In being derived from 15 ever, the scp client only aversal attacks are overwrite arbitrary files server can manipulate
EVE-2021-4 Exclusion Rea NOTIMPLEMEN EVE-2021-4 EVE-2019-6	4224 6.4111 5.4	4 80 ht	mod_apreq2-20090110/2.8.0 mod_perl/2.0.11 Perl/v5.22.2)  tp	2022-02-27 2022-03- 2022-02-27 2023-05-	(r:parsebody() called from Lua s vulnerability though it might be p and earlier.  14 A crafted URI sent to httpd conf (NULL pointer dereference) or, can allow for requests to be dire Request Forgery). This issue at 06 An issue was discovered in Opr rcp, the server chooses which find performs cursory validation of the prevented). A malicious scp ser the scp client target directory. If subdirectories as well (for exam 06 sshd in OpenSSH before 7.4 all dereference and daemon crash	scripts). The Apossible to craft igured as a for for configuratic extend to a decl. ffects Apache lensSH 7.9. Dulles/directories he object name ver (or Man-in recursive open pulpe, to overwind lows remote at 0) via an out-of-	pache httpd t one. This is ward proxy ons mixing for ared Unix Do HTTP Serve the to the scp are sent to to e returned (of -The-Middle ration (-r) is te the .ssh/a ttackers to ca	team is not aw ssue affects Ap (ProxyRequesi rrward and rev omain Socket of r 2.4.7 up to 2. implementatio the client. How nly directory tr attacker) can - performed, the uuthorized_key ause a denial of	vare of an exploit for the bache HTTP Server 2.4 its on) can cause a crasserse proxy declarations endpoint (Server Side 4.51 (included).  In being derived from 15 ever, the scp client only aversal attacks are overwrite arbitrary files is server can manipulate s file).  In service (NULL pointer)
CVE-2021-4 Exclusion Rea	NTED 4224 6.4224	4 80 ht 8 357 ss	mod_apreq2-20090110/2.8.0 mod_perl/2.0.11 Perl/v5.22.2)  tp	2022-02-27 2022-03- 2022-02-27 2023-05- 2022-02-27 2023-05-	(r:parsebody() called from Lua s vulnerabilty though it might be p and earlier.  14 A crafted URI sent to httpd conf (NULL pointer dereference) or, can allow for requests to be dire Request Forgery). This issue at 06 An issue was discovered in Oproce, the server chooses which fiperforms cursory validation of the prevented). A malicious scp ser the scp client target directory. If subdirectories as well (for examons of the prevented) of the prevented of the preve	scripts). The A possible to craft figured as a for for configuratic acted to a decl ffects Apache I enSSH 7.9. Du illes/directories ne object name ver (or Man-in recursive oper ple, to overwri lows remote at o) via an out-of- f packet.c. ftp-server.c in	pache httpd t one. This is ward proxy ons mixing for ared Unix Di- HTTP Serve the to the scp are sent to returned (or The-Middle tation (-f) is te the .ssh/a tackers to or sequence N	team is not awassue affects Ap (ProxyRequesi orward and rev omain Socket of 2.4.7 up to 2. implementatio the client. How only directory tr attacker) can - performed, the uthorized_key ause a denial of EWKEYS mes efore 7.6 does	rare of an exploit for the bache HTTP Server 2.4. Its on) can cause a crast erse proxy declarations endpoint (Server Side 4.51 (included). In being derived from 15 ever, the scp client only aversal attacks are overwrite arbitrary files is server can manipulate is file). If service (NULL pointer sage, as demonstrated not properly prevent wr
EXCLUSION REAL NOTIMPLEMENT CVE-2021-4  CVE-2019-6  CVE-2016-1	NTED 4224 6.4224	4 80 ht 8 357 ss	mod_apreq2-20090110/2.8.0 mod_perl/2.0.11 Perl/v5.22.2)  tp	2022-02-27 2022-03- 2022-02-27 2023-05- 2022-02-27 2023-05-	(r:parsebody() called from Lua s vulnerability though it might be p and earlier.  14 A crafted URI sent to httpd conf (NULL pointer dereference) or, can allow for requests to be dire Request Forgery). This issue at 06 An issue was discovered in Opr rcp, the server chooses which f performs cursory validation of the prevented). A malicious scp ser the scp client target directory. If subdirectories as well (for exam 06 sshd in OpenSSH before 7.4 all dereference and daemon crash Honggfuzz, related to kex.c and	scripts). The A possible to craft figured as a for for configuratic acted to a decl ffects Apache I enSSH 7.9. Du illes/directories ne object name ver (or Man-in recursive oper ple, to overwri lows remote at o) via an out-of- f packet.c. ftp-server.c in	pache httpd t one. This is ward proxy ons mixing for ared Unix Di- HTTP Serve the to the scp are sent to returned (or The-Middle tation (-f) is te the .ssh/a tackers to or sequence N	team is not awassue affects Ap (ProxyRequesi orward and rev omain Socket of 2.4.7 up to 2. implementatio the client. How only directory tr attacker) can - performed, the uthorized_key ause a denial of EWKEYS mes efore 7.6 does	rare of an exploit for the bache HTTP Server 2.4 its on) can cause a crasi erse proxy declarations endpoint (Server Side 4.51 (included). In being derived from 15 ever, the scp client only aversal attacks are overwrite arbitrary files server can manipulate is file). If service (NULL pointer sage, as demonstrated not properly prevent with and the same and the same are the same are the the same are the same are the the same are the same are the same are the same are the the same are the same are the the same are the same are the same are the the same are the same are the the same are the the same are the the same are the the same are the the the the the the the th
CVE-201-4 Exclusion Rea NOTIMPLEMEN CVE-2021-4 CVE-2019-6 CVE-2016-1 CVE-2017-1	Son: WTED 44224 6.44224 6.4111 5.4111	4 80 hi 8 357 se 0 357 se	mod_apreq2-20090110/2.8.0 mod_perl/2.0.11 Perl/v5.22.2)  tp	2022-02-27 2022-03- 2022-02-27 2023-05- 2022-02-27 2023-05- 2022-02-27 2023-05-	(r:parsebody() called from Lua s vulnerability though it might be p and earlier.  14 A crafted URI sent to httpd conf (NULL pointer dereference) or, can allow for requests to be dire Request Forgery). This issue af 06 An issue was discovered in Opr rcp, the server chooses which f performs cursory validation of the prevented). A malicious scp ser the scp client target directory. If subdirectories as well (for exam 06 shd in OpenSSH before 7.4 all dereference and daemon crash Honggfuzz, related to kex.c and 06 The process_open function in soperations in readonly mode, w 06 OpenSSH through 7.7 is prone invalid authenticating user until	scripts). The Apossible to craft igured as a for for configuratic ected to a decl. ffects Apache I enSSH 7.9. Duiles/directories ne object name ver (or Man-in recursive operple, to overver at a) via an out-of-d packet.c. ftp-server.c in hinch allows at to a user enun after the packet read to a user enun after the packet.	pache httpd t one. This is ward proxy one mixing for any one mixing for the transport of the transport to the scp are sent to to e returned (or -The-Middle ration (-r) is te the .ssh/or tackers to or sequence N	team is not awassue affects Ar (ProxyRequesionward and revormain Socket of 2.4.7 up to 2. implementation the client. How mily directory trattacker) can operformed, the uthorized_key ause a denial of EWKEYS mesente zero-lengt uthorized the trequest his to the request his source and the control of the contr	rare of an exploit for the bache HTTP Server 2.4 is on) can cause a crasierse proxy declarations endpoint (Server Side 4.51 (included).  In being derived from 15 ever, the scp client only aversal attacks are overwrite arbitrary files is server can manipulate s file).  In service (NULL pointer stage, as demonstrated not properly prevent with files.
EVE-2021-4 EXCUSION REAL PARTIES OF THE PARTIES OF	\$\text{3.50}\$ \$\text{4224} & 6.\$ \$\text{4224} & 6.\$ \$\text{4111} & 5.\$ \$\text{40708} &	4 80 hi 8 357 ss 0 357 ss 0 357 ss	mod_apreq2-20090110/2.8.0 mod_perl/2.0.11 Perl/v5.22.2)  tp	2022-02-27 2022-03- 2022-02-27 2023-05- 2022-02-27 2023-05- 2022-02-27 2023-05-	(r:parsebody() called from Lua s vulnerability though it might be p and earlier.  14 A crafted URI sent to httpd conf (NULL pointer dereference) or, can allow for requests to be dire Request Forgery). This issue at 06 An issue was discovered in Opr rcp, the server chooses which fine performs cursory validation of the prevented). A malicious scp ser the scp client target directory. If subdirectories as well (for exam of sshd in OpenSSH before 7.4 all dereference and daemon crash Honggfuzz, related to kex.c and 06 The process_open function in soperations in readonly mode, w	scripts). The A possible to craf figured as a for for configuratic acted to a decl ffects Apache I enSSH 7.9. Du illes/directories ne object name ver (or Man-in recursive ope- ple, to overviri lows remote at ) da an out-of- p acket.c. ftp-server.c in hich allows att to a user enun after the pack ostbased.c, and	pache httpd t one. This i ward proxy ons mixing fe ared Unix D HTTP Serve te to the scp are sent to returned (c -The-Middle ration (r) is te the .ssh/a tackers to ca sequence N OpenSSH b ackers to crontaining te containing te containing te containing d auth2-publid	team is not awassue affects Ap (ProxyRequesinward and rev omain Socket of 2.4.7 up to 2. implementatio the client. How hill directory tr attacker) can - performed, the uithorized_key ause a denial of EWKEYS mes efore 7.6 does peate zero-lengt were all the control of the treatment of the control of the control of the control of the treatment of the control of the control of the control of the treatment of the control of the control of the control of the treatment of the control of the control of the control of the treatment of the control of the control of the control of the control of the treatment of the control of the contro	rare of an exploit for the bache HTTP Server 2.4 its on) can cause a crasi erse proxy declarations endpoint (Server Side 4.51 (included). In being derived from 15 eveer, the scp client only aversal attacks are overwrite arbitrary files server can manipulate is file). If service (NULL pointer isage, as demonstrated not properly prevent with files. In ont delaying bailout fo as been fully parsed,
EVE-2021-4 EXCUSION REAL PARTIES PARTI	\$\text{3.50}\$ \$\text{4224} & 6.\$ \$\text{4224} & 6.\$ \$\text{4111} & 5.\$ \$\text{40708} &	4 80 hi 8 357 ss 0 357 ss 0 357 ss	mod_apreq2-20090110/2.8.0 mod_perl/2.0.11 Perl/v5.22.2)  tp	2022-02-27 2022-03- 2022-02-27 2023-05- 2022-02-27 2023-05- 2022-02-27 2023-05-	(r:parsebody() called from Lua s vulnerabilty though it might be p and earlier.  14 A crafted URI sent to httpd conf (NULL pointer dereference) or, can allow for requests to be dire Request Forgery). This issue at 06 An issue was discovered in Opercp, the server chooses which f performs cursory validation of the prevented). A malicious scp ser the scp client target directory. If subdirectories as well (for examons shading for examons for the process_open function in soperations in readonly mode, with the process_open function in soperations in readonly mode, with the process_open function in soperations in readonly mode, with the process_open function in soperations in readonly mode, with the process_open function in soperations in readonly mode, with the process_open function in soperations in readonly mode, with the process_open function in soperations in readonly mode, with the process_open function in soperations in readonly mode, with the process_open function in soperations in readonly mode, with the process_open function in soperations in readonly mode, with the process_open function in soperations in readonly mode, with the process_open function in soperations in readonly mode, with the process_open function in soperations in readonly mode, with the process_open function in soperations in readonly mode, with the process_open function in soperations in readonly mode, with the process_open function in soperations in readonly mode, with the process_open function in soperations in readonly mode, with the process_open function in some pr	scripts). The A possible to craf figured as a for for configuratic screted to a decleffects Apache I enSSH 7.9. Duiles/directories ne object namever (or Man-in recursive open ple, to overwriblows remote at ) via an out-of-d packet.c. ftp-server.c in hich allows att to a user enum after the pack ostbased.c, and r in auth-gss2. uusers on a tar und that the Opt	pache httpd t one. This i ward proxy ons mixing fe arred Unix D- HTTP Serve to the scp are sent to returned (c. The-Middle ration (-f) is to the .sshke tackers to consequence No OpenSSH b ackers to containing d auth2-public in OpenSSH b get system vents server to containing	team is not awassue affects Ar (ProxyRequestorward and revormain Socket of 2.4.7 up to 2. implementation the client. Howard in the client, Howard in the	rare of an exploit for the backe HTTP Server 2.4. Its on) can cause a crasterse proxy declarations endpoint (Server Side 4.51 (included).  In being derived from 19 ever, the scp client only aversal attacks are overwrite arbitrary files is server can manipulate sile). In service (NULL pointer stage, as demonstrated not properly prevent with files.  In on ot delaying bailout foas been fully parsed, could be used by remotin use. NOTE: the
EVE-201-4 Exclusion Rea NOTIMPLEMEN EVE-2021-4 EVE-2019-6 EVE-2016-1 EVE-2017-1 EVE-2018-1	4224 6.4 4111 5.4 6708 5.4 6708 5.4 6709 5.4 6709 5.4	4 80 ht 8 357 ss 0 357 ss 0 357 ss 0 357 ss 0 357 ss	mod_apreq2-20090110/2.8.0 mod_perl/2.0.11 Perl/v5.22.2)  tp	2022-02-27 2023-05- 2022-02-27 2023-05- 2022-02-27 2023-05- 2022-02-27 2023-05- 2022-02-27 2023-05-	(r:parsebody) called from Lua s vulnerability though it might be pand earlier.  14 A crafted URI sent to httpd conf (NULL pointer dereference) or, can allow for requests to be dire Request Forgery). This issue at 06 An issue was discovered in Opercp, the server chooses which fiperforms cursory validation of it prevented). A malicious scp ser the scp client target directory. If subdirectories as well (for exam 06 sshd in OpenSSH before 7.4 all dereference and daemon crash Honggfuzz, related to kex.c and 07 The process_open function in soperations in readonly mode, we 06 OpenSSH through 7.7 is prone invalid authenticating user until related to auth2-gss.c, auth2-hd of Remotely observable behavioun attackers to detect existence of discoverer states We understat username enumeration (or "ora 06 sshd in OpenSSH 6.2 through 8 allows privilege escalation becaprograms for AuthorizedKeysCd associated with group members	scripts). The Alpossible to craftigured as a for for configuratic screed to a decleffects Apache I enSSH 7.9. Dulles/directories ne object name ver (or Man-in recursive open pile, to overwriblows remote at ) via an out-of-of-of-of-of-of-of-of-of-of-of-of-of-	pache httpd t one. This i ward proxy ns mixing fe ared Unix Di HTTP Serve te to the scp are sent to to the scp the sch tackers to co sequence N  OpenSSH b ackers to co sequence N  OpenSSH b ac	team is not awassue affects AproxyRequest invard and revorant not be a continued in the client. How the client had been also been as a denial of EWKEYS messer of 2.4.7 to the client of the client in	rare of an exploit for the bache HTTP Server 2.4 is on) can cause a crasierse proxy declarations endpoint (Server Side 4.51 (included).  In being derived from 19 ever, the scp client only aversal attacks are overwrite arbitrary files is server can manipulate is file).  In service (NULL pointer sage, as demonstrated not properly prevent with files.  In on other delaying bailout for as been fully parsed, could be used by remotin use. NOTE: the avant to treat such a onfigurations are used, ed as expected. Helper and may run with privile and may run with privile and crasing a server of the care of the c
CVE-201-4 Exclusion Rea NOTIMPLEMEN CVE-2021-4 CVE-2019-6 CVE-2016-1 CVE-2017-1 CVE-2018-1 CVE-2018-1	1111 5.1 1111 5.1	4 80 ht 8 357 ss 0 357 ss 0 357 ss 0 357 ss 4 357 ss	mod_apreq2-20090110/2.8.0 mod_perl/2.0.11 Perl/v5.22.2)  tp	2022-02-27 2023-05- 2022-02-27 2023-05- 2022-02-27 2023-05- 2022-02-27 2023-05- 2022-02-27 2023-05- 2022-02-27 2023-05-	(r:parsebody() called from Lua s vulnerability though it might be pand earlier.  14 A crafted URI sent to httpd conf (NULL pointer dereference) or, can allow for requests to be dire Request Forgery). This issue at 06 An issue was discovered in Opercp, the server chooses which fiperforms cursory validation of the prevented). A malicious scp ser the scp client target directory. If subdirectories as well (for examone shadown) and the subdirectories as well (for examone shadown) and the subdirectories as well (for examone shadown). The process_open function in soperations in readonly mode, wo 06 OpenSSH through 7.7 is prone invalid authenticating user until related to auth2-gss.c, auth2-ho. 66 Remotely observable behaviour attackers to detect existence of discoverer states "We understat username enumeration (or "ora 06 sshd in OpenSSH 6.2 through 6 allows privilege escalation becaprograms for AuthorizedKeysCo."	scripts). The Apossible to craftigured as a for for configuratic ected to a decle fects Apache I en SSH 7.9. Dulles/directories ne object name ver (or Man-in recursive operable), to overwritows remote at ) via an out-of-I packet.c. fftp-server.c in hich allows att to a user enun after the packet of the packet	pache httpd t one. This is ward proxy ons mixing fe ared Unix Do HTTP Serve te to the scp are sent to to returned (o,-The-Middle ration (-r) is te the .ssh/a tackers to co sequence N OpenSSH b ackers to or areation vulr et containing d auth2-publ c in OpenSS get system v ensSH deve erability. when certain tal groups. withorizedPr nd process, i as an Obser as an Ob	team is not awassue affects AproxyRequest invard and revomain Socket of 2.4.7 up to 2. implementation the client. How the client How the clie	rare of an exploit for the bache HTTP Server 2.4. Its on) can cause a crasterse proxy declarations endpoint (Server Side 4.51 (included).  In being derived from 19 ever, the scp client only aversal attacks are overwrite arbitrary files is sacready and the state of the scale of the service (NULL pointer stage, as demonstrated not properly prevent with files.  In ond delaying bailout for as been fully parsed, could be used by remotinuse. NOTE: the want to treat such a onfigurations are used, ed as expected. Helper and may run with privile tion specifies running the uncy leading to an dle attackers to target in uncy leading to an office and the same to target in uncy leading to an office attackers to target in uncy leading to an office attackers to target in uncy leading to an office attackers to target in uncy leading to an office attackers to target in the same provided as taken to target in uncy leading to an office attackers to target in the same provided and the same provided as the same provided and the same provided as
EXCUSION Rea EXCUSION REA NOTIMPLEMEN CVE-2021-4 CVE-2019-6	5000 5.1 5906 5.1 5919 5.1 61617 4.1	4 80 ht 8 357 ss 0 357 ss 0 357 ss 0 357 ss 4 357 ss	mod_apreq2-20090110/2.8.0 mod_perl/2.0.11 Perl/v5.22.2)  tp	2022-02-27 2023-05- 2022-02-27 2023-05- 2022-02-27 2023-05- 2022-02-27 2023-05- 2022-02-27 2023-05- 2022-02-27 2023-05-	(r:parsebody() called from Lua s vulnerability though it might be pand earlier.  14 A crafted URI sent to httpd conf (NULL pointer dereference) or, can allow for requests to be dire Request Forgery). This issue at 06 An issue was discovered in Opr rcp, the server chooses which fiperforms cursory validation of the prevented). A malicious scp ser the scp client target directory. If subdirectories as well (for exam of shading) of the school of the school of the school of the prevented). A malicious scp ser the scp client target directory. If subdirectories as well (for exam of shading) of the school of the prevented of the school of the process_open function in soperations in readonly mode, we of OpenSSH through 7.7 is prone invalid authenticating user until related to auth2-gss.c, auth2-hc of Remotely observable behavious attackers to detect existence of discoverer states We understate username enumeration (or "ora allows privilege escalation becaprograms for AuthorizedKeysCr associated with group members command as a different user.  106 The client side in OpenSSH 5.7 information leak in the algorithm connection attempts (where no	scripts). The A possible to craf figured as a for for configuratic acted to a decl ffects Apache I enSSH 7.9. Du illes/directories ne object name ver (or Man-in recursive ope- ple, to overviri lows remote at ) y aan out-of- ) packet.c. ftp-server.c in hich allows att to a user enun after the pack postbased.c, and r in auth-gss2.c users on a tar und that the Opc le") as a vuln 3.x before 8.8, uses suppleme ommand and A ships of the ssl through 8.4 h n negotation. The host key for th de also affecter enSSH 7.9. Du Adan-in-The-Mic gar, by using AN	pache httpd t one. This i ward proxy ons mixing fe arred Unix D HTTP Serve te to the scp are sent to returned (c)	team is not awassue affects Ap (ProxyRequesinward and rev omain Socket of 2.4.7 up to 2. implementatio the client. How high directory tr attacker) can - performed, the uthorized_key ause a denial of EWKEYS mes efore 7.6 does pate zero-lengt interesting the control of the client of the client of the control of the control of the control of the control of the configura vable Discrepanan-in-the-midd is been cached character enc o) can employ of oddes to hide ac	rare of an exploit for the bache HTTP Server 2.4 is on) can cause a crasierse proxy declarations endpoint (Server Side 4.51 (included).  In being derived from 19 ever, the scp client only aversal attacks are overwrite arbitrary files is server can manipulate is file).  In service (NULL pointer sage, as demonstrated not properly prevent with files.  In ont delaying bailout foas been fully parsed, could be used by remoting use. NOTE: the want to treat such a onfigurations are used, ed as expected. Helper and may run with privile tion specifies running thancy leading to an dle attackers to target in by the client). NOTE: so oding in the progress trafted object names to

# 192.168.2.150 Hostname Operating System OS Version CPE NIC Vendor Motorola Mobility LLC a Lenovo Company First Seen 2022-03-02 2023-05-06 Last Seen Critical CVSS HIGH CVSS MEDIUM CVSS LOW CVSS CVSS Total NumberProtocolServiceService Version53794tcpsipZoiper rv2.10.4.4 (Status: 200 OK)53795tcptcpwrappedShowing 2 results. CPE Has Exploits? Verified Service Verified Version First Seen Last Seen 2023-05-06 2023-05-06 2023-05-06 2023-05-06

ostname											
perating Sys	tem Fr	eeRS	:D								
	teili Fi	еевз	טו								
S Version											
PE	ср	e:/o:f	reebs	d:freek	osd						
IC Vendor	(T	p-link	Tech	nologie	es)						
rst Seen	20	22-02	2-27								
ast Seen	20	23-05	5-06								
ritical CVSS											
IGH CVSS											
EDIUM CVSS	18	3									
ow cvss	6										
VSS Total	24	ı									
orts Numbe	er Prot	tocol	Serv	rice S	ervice Version		CPE	Has Exploits?	Verified Service	Verified Version	First Seen Last See
22 80	tcp tcp		ssh http		penSSH 7.9 (FreeBSD 202 pache httpd 2.4.48 ((FreeB		cpe:/a:openbsd:openssh:7.9: cpe:/a:apache:http_server:2.4.48	Yes		Apache 2.4.56	2022-02-27 2023-05- 2022-02-27 2023-05-
123	udp		ntp?	P	erl/v5.32.1)	,		1			2023-04-27 2023-05
Showin		ults.									
/E Scores											
CVE	C	cvss	Port	Servi	ce Service Version	First Seen Last Seen	Description				
CVE-2021-39 Exclusion Reas	son:	<del>7.5</del>	80	http	Apache httpd 2.4.48 ((FreeBSD) mod_perl/2.0.11	2022-02-27 2023-05-06	ap_escape_quotes() may write beyon pass untrusted data to these function Server 2.4.48 and earlier.				
CVE-2021-4	4790	<del>7.5</del>	80	httn	Perl/v5.32.1) Apache httpd 2.4.48	2022-02-27 2023-05-06	A carefully crafted request body can	r cause a huffer o	verflow in the m	nd lua multinart n	narser (r:narsehody/)
Exclusion Reas	son:	1.5		пцр	((FreeBSD) mod_perl/2.0.11	2022 02 27 2020 00 00	called from Lua scripts). The Apache possible to craft one. This issue affe	e httpd team is no	ot aware of an ex	ploit for the vulne	
CVE-2022-22		7.5	80	http	Perl/v5.32.1) Apache httpd 2.4.48 ((FreeBSD)	2023-04-27 2023-05-06	Apache HTTP Server 2.4.52 and ea discarding the request body, exposir				are encountered
WRONGVERS					mod_perl/2.0.11 Perl/v5.32.1)				1		
CVE-2022-23	3943	7.5	80	http	Apache httpd 2.4.48	2023-04-27 2023-05-06	Out-of-bounds Write vulnerability in				
Exclusion Reas					((FreeBSD) mod_perl/2.0.11 Perl/v5.32.1)		memory with possibly attacker proving prior versions.	ded data. This iss	sue affects Apac	he HTTP Server	2.4 version 2.4.52 and
CVE-2022-3:	1813	7.5	80	http	Apache httpd 2.4.48	2023-04-27 2023-05-06	Apache HTTP Server 2.4.53 and ea	rlier may not send	d the X-Forward	ed-* headers to th	ne origin server based o
Exclusion Reas	son:			пар	((FreeBSD) mod_perl/2.0.11	2020 0 1 2 2020 00 00	client side Connection header hop-b the origin server/application.				
CVE-2021-40	0438	6.8	80	http	Perl/v5.32.1) Apache httpd 2.4.48 ((FreeBSD) mod_perl/2.0.11	2022-02-27 2023-05-06	A crafted request uri-path can cause remote user. This issue affects Apac				ver choosen by the
CVE-2021-4	4224	6.4	80	http	Perl/v5.32.1) Apache httpd 2.4.48 ((FreeBSD)	2022-02-27 2023-05-06	A crafted URI sent to httpd configure dereference) or, for configurations m	nixing forward and	d reverse proxy	declarations, can	allow for requests to be
CVE-2022-28	8615	6.4	80	httn	mod_perl/2.0.11 Perl/v5.32.1) Apache httpd 2.4.48	2023-04-27 2023-05-06	directed to a declared Unix Domain HTTP Server 2.4.7 up to 2.4.51 (incl Apache HTTP Server 2.4.53 and ea	luded).	•		·
0 V L 2022 2	3013	0.4	00	тер	((FreeBSD) mod_perl/2.0.11 Perl/v5.32.1)	2020 04 27 2020 00 00	ap_strcmp_match() when provided varieties appeared into such a cathypothetically be affected.	with an extremely	large input buffe	er. While no code	distributed with the
CVE-2019-6:	111	5.8	22	ssh	OpenSSH 7.9 (FreeBSD 20200214; protocol 2.0)	2022-02-27 2023-05-06	An issue was discovered in OpenSS server chooses which files/directorie validation of the object name returne Man-in-The-Middle attacker) can ow (-r) is performed, the server can mai .ssh/authorized_keys file).	es are sent to the ed (only directory erwrite arbitrary fi	client. However, traversal attacks les in the scp cli	the scp client on are prevented). ent target directo	ly performs cursory A malicious scp server ry. If recursive operation
CVE-2022-22	2721	5.8	80	http	Apache httpd 2.4.48 ((FreeBSD) mod_perl/2.0.11 Perl/v5.32.1)	2023-04-27 2023-05-06	If LimitXMLRequestBody is set to all integer overflow happens which late 2.4.52 and earlier.				
CVE-2021-3	3193	5.0	80	http	Apache httpd 2.4.48 ((FreeBSD) mod_perl/2.0.11 Perl/v5.32.1)	2022-02-27 2023-05-06	A crafted method sent through HTTF request splitting or cache poisoning.				
CVE-2021-34	4798	5.0	80	http	Apache httpd 2.4.48 ((FreeBSD) mod_perl/2.0.11 Perl/v5.32.1)	2022-02-27 2023-05-06	Malformed requests may cause the Server 2.4.48 and earlier.	server to derefere	ence a NULL po	inter. This issue a	ffects Apache HTTP
CVE-2021-30	6160	5.0	80	http	Apache httpd 2.4.48 ((FreeBSD) mod_perl/2.0.11 Perl/v5.32.1)	2022-02-27 2023-05-06	A carefully crafted request uri-path of (DoS). This issue affects Apache HT				ocated memory and cra
CVE-2022-22	2719	5.0	80	http	Apache httpd 2.4.48 ((FreeBSD) mod_perl/2.0.11 Perl/v5.32.1)	2023-04-27 2023-05-06	A carefully crafted request body can crash. This issue affects Apache HT			ory area which cou	uld cause the process t
CVE-2022-20	6377	5.0	80	http	Apache httpd 2.4.48 ((FreeBSD) mod_perl/2.0.11 Perl/v5.32.1)	2023-04-27 2023-05-06	Inconsistent Interpretation of HTTP I Apache HTTP Server allows an atta issue affects Apache HTTP Server A	cker to smuggle r	equests to the A	JP server it forwa	ards requests to. This
CVE-2022-28	8614	5.0	80	http	Apache httpd 2.4.48 ((FreeBSD) mod_perl/2.0.11 Perl/v5.32.1)	2023-04-27 2023-05-06	The ap_rwrite() function in Apache I can cause the server to reflect very function. Modules compiled and dist function and may pass it a very large resolve the issue.	large input using ributed separately	ap_rwrite() or ap y from Apache H	_rputs(), such as	with mod_luas r:puts() use the 'ap_rputs'

CVE-2022-29404	5.0	80	http	Apache httpd 2.4.48 ((FreeBSD) mod_perl/2.0.11 Perl/v5.32.1)	2023-04-27 2023-05-06 In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.
CVE-2022-30556	5.0	80	http	Apache httpd 2.4.48 ((FreeBSD) mod_perl/2.0.11 Perl/v5.32.1)	2023-04-27 2023-05-06 Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.
CVE-2019-16905	4.4	22	ssh	OpenSSH 7.9 (FreeBSD 20200214; protocol 2.0)	2022-02-27 2023-05-06 OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre- authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.
CVE-2021-41617	4.4	22	ssh	OpenSSH 7.9 (FreeBSD 20200214; protocol 2.0)	2022-02-27 2023-05-06 sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.
CVE-2020-14145	4.3	22	ssh	OpenSSH 7.9 (FreeBSD 20200214; protocol 2.0)	2022-02-27 2023-05-06 The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.
CVE-2019-6109	4.0	22	ssh	OpenSSH 7.9 (FreeBSD 20200214; protocol 2.0)	2022-02-27 2023-05-06 An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.
CVE-2019-6110 Showing 23 results		22	ssh	OpenSSH 7.9 (FreeBSD 20200214; protocol 2.0)	2022-02-27 2023-05-06 In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.

Showing 23 results.

Note: Low-ranked results are informational-only or otherwise inactionable and are thus excluded from this listing.

192.1	L68.2.167	7						
Hostna	ame	blackpi	3					
Operat	ting Systen							
OS Vei	rsion							
CPE NIC Ve	ndor	(Raspb	orn, F	Di Eoune	lation)			
First S		2022-02	•	r Found	iation)			
Last S		2023-05						
	I CVSS							
HIGH (		18						
LOW	JM CVSS CVSS	6						
cvss		24						
Ports								
rons	Number	Protocol	Serv	ice Se	rvice Version		CPE Has Verified Verified First Seen Last	Seen
	00			-	001170/5 000 000		Exploits? Service Version	05.00
		tcp tcp	ssh http		enSSH 7.9 (FreeBSD 202 ache httpd 2.4.48 ((FreeB		cpe:/a:openbsd:openssh:7.9: Yes 2022-02-27 2023- cpe:/a:apache:http_server:2.4.48: Yes Apache 2.4.56 2022-02-27 2023-	
		юр	Пер		rl/v5.32.1)	55) mod_pen/2.0.11	7-pacific 2-4-30 2022 02 21 2020	05 00
		udp	ntp?	•			2023-04-27 2023-	-05-06
	Showing 3	results.						
CVE So								
CVE	: -2021-3927		80		e Service Version Apache httpd 2.4.48	First Seen Last Seen	n Description 16 ap escape quotes() may write beyond the end of a buffer when given malicious input. No included module	96
Exc	clusion Reason: RONGVERSION	3 7.3	00	пцр	((FreeBSD) mod_perl/2.0.11 Perl/v5.32.1)	2022-02-27 2023-03-00	pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache H Server 2.4.48 and earlier.	
	-2021-4479	7. <del>5</del>	80	http	Apache httpd 2.4.48	2022-02-27 2023-05-06	6 A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody()	
	clusion Reason: TIMPLEMENTED				((FreeBSD) mod_perl/2.0.11 Perl/v5.32.1)		called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it mig possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.	int be
Exc	E-2022-2272 clusion Reason: RONGVERSION		80	http	Apache httpd 2.4.48 ((FreeBSD) mod_perl/2.0.11 Perl/v5.32.1)	2023-04-27 2023-05-06	6 Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling	
Exc	-2022-2394 clusion Reason: RONGVERSION		80	http	Apache httpd 2.4.48 ((FreeBSD) mod_perl/2.0.11	2023-04-27 2023-05-06	6 Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 at prior versions.	
Exc	E-2022-3181 clusion Reason:		80	http	Perl/v5.32.1)  Apache httpd 2.4.48 ((FreeBSD) mod_perl/2.0.11	2023-04-27 2023-05-06	6 Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded.* headers to the origin server base client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authenticatio the origin server/application.	
	E-2021-4043		80	http	Perl/v5.32.1) Apache httpd 2.4.48 ((FreeBSD)	2022-02-27 2023-05-06	6 A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.	
CVE	E-2021-4422	24 6.4	80	http	mod_perl/2.0.11 Perl/v5.32.1) Apache httpd 2.4.48	2022-02-27 2023-05-06	.  6 A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL po	ointer
					((FreeBSD) mod_perl/2.0.11 Perl/v5.32.1)		dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apa HTTP Server 2.4.7 up to 2.4.51 (included).	
CVE	-2022-2861	15 6.4	80	http	Apache httpd 2.4.48 ((FreeBSD) mod_perl/2.0.11 Perl/v5.32.1)	2023-04-27 2023-05-06	6 Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.	
CVE	-2019-6111	5.8	22	ssh	OpenSSH 7.9 (FreeBSD 20200214; protocol 2.0)	2022-02-27 2023-05-06	6 An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp sen Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive opera (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized keys file).	rver (o
CVE	-2022-2272	5.8	80	http	Apache httpd 2.4.48 ((FreeBSD) mod_perl/2.0.11 Perl/v5.32.1)	2023-04-27 2023-05-06	6 If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systen integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.	
CVE	-2021-3319	93 5.0	80	http	Apache httpd 2.4.48 ((FreeBSD) mod_perl/2.0.11 Perl/v5.32.1)	2022-02-27 2023-05-06	6 A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can be request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.	lead to
CVE	E-2021-3479	98 5.0	80	http	Apache httpd 2.4.48 ((FreeBSD) mod_perl/2.0.11 Perl/v5.32.1)	2022-02-27 2023-05-06	6 Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.	5
CVE	-2021-3616	5.0	80	http	Apache httpd 2.4.48 ((FreeBSD) mod_perl/2.0.11 Perl/v5.32.1)	2022-02-27 2023-05-06	6 A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and (DoS). This issue affects Apache HTTP Server versions 2.4.30 to 2.4.48 (inclusive).	crash
CVE	E-2022-2271	19 5.0	80	http	Apache httpd 2.4.48 ((FreeBSD) mod_perl/2.0.11 Perl/v5.32.1)	2023-04-27 2023-05-06	6 A carefully crafted request body can cause a read to a random memory area which could cause the proces crash. This issue affects Apache HTTP Server 2.4.52 and earlier.	ss to
CVE	-2022-2637	77 5.0	80	http	Apache httpd 2.4.48 ((FreeBSD) mod_perl/2.0.11 Perl/v5.32.1)	2023-04-27 2023-05-06	6 Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp. Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. Thi issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.	
CVE	-2022-2861	5.0	80	http	Apache httpd 2.4.48 ((FreeBSD) mod_perl/2.0.11 Perl/v5.32.1)	2023-04-27 2023-05-06	6 The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an atta can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:put function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers resolve the issue.	uts()

CVE-2022-29404	5.0	80	http	Apache httpd 2.4.48 ((FreeBSD) mod_perl/2.0.11 Perl/v5.32.1)	2023-04-27 2023-05-06 In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.
CVE-2022-30556	5.0	80	http	Apache httpd 2.4.48 ((FreeBSD) mod_perl/2.0.11 Perl/v5.32.1)	2023-04-27 2023-05-06 Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.
CVE-2019-16905	4.4	22	ssh	OpenSSH 7.9 (FreeBSD 20200214; protocol 2.0)	2022-02-27 2023-05-06 OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre- authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.
CVE-2021-41617	4.4	22	ssh	OpenSSH 7.9 (FreeBSD 20200214; protocol 2.0)	2022-02-27 2023-05-06 sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedFrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.
CVE-2020-14145	4.3	22	ssh	OpenSSH 7.9 (FreeBSD 20200214; protocol 2.0)	2022-02-27 2023-05-06 The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.
CVE-2019-6109	4.0	22	ssh	OpenSSH 7.9 (FreeBSD 20200214; protocol 2.0)	2022-02-27 2023-05-06 An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.
CVE-2019-6110 Showing 23 results		22	ssh	OpenSSH 7.9 (FreeBSD 20200214; protocol 2.0)	2022-02-27 2023-05-06 In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.

Showing 23 results.

Note: Low-ranked results are informational-only or otherwise inactionable and are thus excluded from this listing.

# 192.168.2.171 Hostname Operating System OS Version CPE NIC Vendor First Seen 2023-04-26 Last Seen 2023-05-06 Critical CVSS HIGH CVSS MEDIUM CVSS LOW CVSS CVSS Total

# 192.168.2.172 Hostname Operating System OS Version CPE (Samsung Electronics) 2023-04-26 NIC Vendor First Seen 2023-05-06 Last Seen Critical CVSS HIGH CVSS MEDIUM CVSS LOW CVSS CVSS Total Number Protocol Service Service Version 60624 tcp sip Zoiper v2.10.19.6 (Status: 200 OK) 60625 tcp tcpwrapped Showing 2 results. Topic value CPE Has Exploits? Verified Service Verified Version First Seen Last Seen 2023-05-06 2023-05-06 2023-05-06 2023-05-06

# 192.168.2.174 Hostname Operating System OS Version CPE NIC Vendor First Seen 2023-04-27 Last Seen 2023-05-06 Critical CVSS HIGH CVSS MEDIUM CVSS LOW CVSS CVSS Total

## 192.168.2.185 Hostname slack15pve2 Operating System OS Version CPE NIC Vendor First Seen 2023-04-26 2023-05-06 Last Seen Critical CVSS HIGH CVSS MEDIUM CVSS LOW CVSS CVSS Total CPE Has Exploits? Verified Service Verified Version First Seen Last Seen Number Protocol Service Service Version 22 tcp ssh OpenSSH 9.3 (protocol 2.0) 25 tcp smtp Postfix smtpd 80 tcp http Apache httpd 2.4.57 ((Unix)) 161 udp snmp SNMPv1 server; net-snmp SNMPv3 server (public) 2023-04-27 2023-05-06 2023-04-27 2023-05-06 2023-04-27 2023-05-06 2023-04-27 2023-05-06 Showing 4 results.

## 192.168.2.186 Hostname devuanraid Operating System Linux OS Version CPE cpe:/o:linux:linux\_kernel NIC Vendor (Ubiquiti Networks) First Seen 2023-04-26 2023-05-06 Last Seen Critical CVSS HIGH CVSS MEDIUM CVSS LOW CVSS CVSS Total Number Protocol Service Service Version CPE Has Exploits? Verified Service Verified Version First Seen Last Seen 22 tcp ssh Dropbear sshd 2013.59 (protocol 2.0) Showing 1 results. 2023-04-27 2023-05-06

### 192.168.2.188 Hostname Operating System OS Version CPE NIC Vendor First Seen 2023-04-26 Last Seen 2023-05-06 Critical CVSS HIGH CVSS MEDIUM CVSS LOW CVSS CVSS Total Ports Number Protocol Service Service Version CPE Has Exploits? Verified Service Verified Version First Seen Last Seen udp zeroconf tcp tcpwrapped 5353 2023-04-27 2023-04-27 2023-04-27 2023-04-27 62078 Showing 2 results.

# 192.168.2.189 Hostname Operating System OS Version CPE NIC Vendor First Seen 2023-04-26 Last Seen 2023-05-06 Critical CVSS HIGH CVSS MEDIUM CVSS LOW CVSS CVSS Total

	tem Un	:0natha nix	ail									
Version	011											
E												
C Vendor												
st Seen	20	22-02	-27									
st Seen		23-05	-06									
tical CVSS	2											
SH CVSS	11 63											
DIUM CVSS W CVSS	21											
SS Total	97											
Number	r Proto	col S	Servic	е :	Service Version			CPE	Has Exploits?	Verified Service	Verified Version	First Seen Last S
21	tcp	ft	р	١	sftpd 3.0.5							2022-03-05 2023-0
25	tcp	SI	mtp	-	Postfix smtpd							2022-02-27 2023-0
53	tcp	de	lomair	n (	unknown banner: A	pache 1.3)						2022-02-27 2023-0
67	udp	dl	hcps									2023-04-27 2023-0
68	udp	dl	hcpc									2023-04-27 2023-0
79	tcp	fir	nger	1	BSD fingerd							2023-04-27 2023-0
80	tcp	ht	ttp			7 ((Unix) PHP/7.4.33						2022-02-27 2023-0
				1	mod_apreq2-20101	207/2.8.1 mod_perl/2.0.1	2 Perl/v5.34.0)					0000
123	udp		tp?		Combo			anaylayaan harranii 100	V-			2023-04-27 2023-0
139	tcp	_			Samba smbd 4.6.2	CNIMPLE		cpe:/a:samba:samba:4.6.2:	Yes			2022-02-27 2023-0
161	udp		nmp		net-snmp; net-snmp							2023-04-27 2023-0
357	tcp		sh	_	OpenSSH 9.3 (proto	ocol 2.0)						2022-02-27 2023-0
445	tcp	_			Samba smbd 4.6.2			cpe:/a:samba:samba:4.6.2:	Yes			2022-02-27 2023-0
1716	tcp		cpwra									2022-02-27 2023-0
5060	udp	_	ip-pro	_	Asterisk PBX 16.12			cpe:/a:digium:asterisk:16.12.0	:			2023-04-27 2023-0
33892	tcp		ns-wb erver	[- '	vіпиаівох vm Rem	ote Desktop Service						2023-04-27 2023-0
Showing	15 resi											
Scores												
	-											
VE	C	vss i	Port	Service	Service Version	First Seen Last Seen	Description					
		_	139	netbios	- Samba smbd	First Seen Last Seen 2022-02-27 2023-05-0	Samba since version	on 3.5.0 and before 4.6.4, 4.5.10				
		_	139				Samba since versio allowing a malicious	on 3.5.0 and before 4.6.4, 4.5.10 s client to upload a shared librar				
CVE-2017-74	194	10.0	139	netbios ssn	- Samba smbd 4.6.2	2022-02-27 2023-05-0	Samba since versionallowing a malicious execute it.	s client to upload a shared libra	ry to a writable	share, and t	hen cause the	e server to load and
CVE-2017-74	194	10.0	139 445	netbios ssn	- Samba smbd	2022-02-27 2023-05-0	Samba since versionallowing a malicious execute it.     Samba since versionallowing a malicious allowing a malicious.		y to a writable  and 4.4.14 is	share, and t	hen cause the	e server to load and e execution vulnerabilit
CVE-2017-74	194 <b>1</b>	10.0	139 445	netbios ssn netbios ssn	- Samba smbd 4.6.2 - Samba smbd 4.6.2	2022-02-27 2023-05-0 2022-02-27 2023-05-0	6 Samba since versio allowing a malicious execute it. 6 Samba since versio allowing a malicious execute it.	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 s client to upload a shared librar	y to a writable  and 4.4.14 is	share, and t	hen cause the	e server to load and e execution vulnerabilit
CVE-2017-74 CVE-2017-74 CVE-2017-74	194 <b>1</b>	10.0	139 445 139	netbios ssn netbios ssn netbios	- Samba smbd 4.6.2 - Samba smbd 4.6.2 - Samba smbd	2022-02-27 2023-05-0 2022-02-27 2023-05-0	6 Samba since versio allowing a malicious execute it. 6 Samba since versio allowing a malicious execute it.	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10	y to a writable  and 4.4.14 is	share, and t	hen cause the	e server to load and e execution vulnerabilit
CVE-2017-74 CVE-2017-74	194 1 194 1 7049	10.0	139 445 139	netbios ssn netbios ssn netbios ssn	- Samba smbd 4.6.2 - Samba smbd 4.6.2 - Samba smbd 4.6.2	2022-02-27 2023-05-0 2022-02-27 2023-05-0 2023-04-27 2023-05-0	6 Samba since versio allowing a malicious execute it. 6 Samba since versio allowing a malicious execute it. 6 Kerberos Security F	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 s client to upload a shared librar Feature Bypass Vulnerability	ry to a writable 0 and 4.4.14 is ry to a writable	share, and t vulnerable to share, and t	hen cause the o remote code hen cause the	e server to load and e execution vulnerabilit e server to load and
CVE-2017-74 CVE-2017-74	194 1 194 1 7049	10.0	139 445 139 139	netbios ssn netbios ssn netbios ssn	- Samba smbd 4.6.2 - Samba smbd 4.6.2 - Samba smbd	2022-02-27 2023-05-0 2022-02-27 2023-05-0 2023-04-27 2023-05-0	Samba since versio allowing a malicious execute it. Samba since versio allowing a malicious execute it. Kerberos Security F A flaw was found in authentication. The	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 is client to upload a shared librar eature Bypass Vulnerability the way Samba, as an Active I Samba AD DC, could become	ry to a writable  and 4.4.14 is  y to a writable  Directory Doma confused abou	share, and to vulnerable to share, and to share, and to share to the share to the share to the user a share to the user a share, and to the user a share to the user a share to the user a share, and the user a share to the user	then cause the o remote code then cause the r, implemented ticket represe	e server to load and e execution vulnerabilit e server to load and d Kerberos name-base nts if it did not strictly
CVE-2017-74 CVE-2017-74 CVE-2020-17	194 1 1494 1 17049 9	10.0 1 10.0 4 9.0 1	139 445 139 139	netbios ssn netbios ssn netbios ssn netbios ssn	- Samba smbd 4.6.2 - Samba smbd 4.6.2 - Samba smbd 4.6.2 - Samba smbd 4.6.2	2022-02-27 2023-05-0 2022-02-27 2023-05-0 2023-04-27 2023-05-0 2022-03-02 2023-05-0	s Samba since versio allowing a malicious execute it. 5 Samba since versio allowing a malicious execute it. 6 Kerberos Security F 6 A flaw was found in authentication. The require a Kerberos	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 s client to upload a shared librar eature Bypass Vulnerability the way Samba, as an Active I Samba AD DC, could become PAC and always use the SIDs f	ry to a writable  and 4.4.14 is  y to a writable  Directory Doma confused abou	share, and to vulnerable to share, and to share, and to share to the share to the share to the user a share to the user a share, and to the user a share to the user a share to the user a share, and the user a share to the user	then cause the o remote code then cause the r, implemented ticket represe	e server to load and e execution vulnerabilit e server to load and d Kerberos name-base nts if it did not strictly
CVE-2017-74 CVE-2017-74 CVE-2020-17	194 1 1494 1 17049 9	10.0 1 10.0 4 9.0 1	139 445 139 139 445	netbios ssn netbios ssn netbios ssn netbios ssn	- Samba smbd 4.6.2 - Samba smbd	2022-02-27 2023-05-0 2022-02-27 2023-05-0 2023-04-27 2023-05-0 2022-03-02 2023-05-0	s Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. 6 Kerberos Security F 5 A flaw was found in authentication. The require a Kerberos	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 is client to upload a shared librar eature Bypass Vulnerability the way Samba, as an Active I Samba AD DC, could become	ry to a writable  and 4.4.14 is  y to a writable  Directory Doma confused abou	share, and to vulnerable to share, and to share, and to share to the share to the share to the user a share to the user a share, and to the user a share to the user a share to the user a share, and the user a share to the user	then cause the o remote code then cause the r, implemented ticket represe	e server to load and e execution vulnerabilit e server to load and d Kerberos name-base nts if it did not strictly
CVE-2017-74 CVE-2017-74 CVE-2020-17 CVE-2020-25	194 1 1494 1 17049 ! 5719 !	10.0 4 10.0 4 9.0 1 9.0 2	139 445 139 139 445	netbios ssn netbios ssn netbios ssn netbios ssn	- Samba smbd 4.6.2	2022-02-27 2023-05-0 2022-02-27 2023-05-0 2023-04-27 2023-05-0 2022-03-02 2023-05-0 2023-04-27 2023-05-0	Samba since versio allowing a malicious execute it. Samba since versio allowing a malicious execute it. Kerberos Security F A flaw was found in authentication. The require a Kerberos Security F Kerberos Security F Kerberos Security F	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 s client to upload a shared librar Feature Bypass Vulnerability the way Samba, as an Active I Samba AD DC, could become PAC and always use the SIDs f Feature Bypass Vulnerability	y to a writable  o and 4.4.14 is y to a writable  Directory Doma confused abou ound within. Th	share, and t vulnerable to share, and t ain Controller to the user a ne result cou	hen cause the o remote code hen cause the r, implemented ticket represe ld include tota	e server to load and e execution vulnerabilit e server to load and d Kerberos name-base nts if it did not strictly al domain compromise
CVE-2017-74 CVE-2017-74 CVE-2020-17 CVE-2020-25	194 1 1494 1 17049 ! 5719 !	10.0 4 10.0 4 9.0 1 9.0 2	139 445 139 139 445 445	netbios ssn netbios ssn netbios ssn netbios ssn	- Samba smbd 4.6.2 - Samba smbd	2022-02-27 2023-05-0 2022-02-27 2023-05-0 2023-04-27 2023-05-0 2022-03-02 2023-05-0 2023-04-27 2023-05-0	S Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. S Kerberos Security F S A flaw was found in authentication. The require a Kerberos S Kerberos Security F S A flaw was found in	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 s client to upload a shared librar eature Bypass Vulnerability the way Samba, as an Active I Samba AD DC, could become PAC and always use the SIDs f	y to a writable  and 4.4.14 is y to a writable  Directory Doma confused abou ound within. The	share, and to vulnerable to share, and to share, and to share ain Controller to the user a ne result could ain Controller ain Controller	hen cause the oremote code then cause the r, implemented ticket represe lid include totar, implemented r, implemented r, implemented r, implemented	e server to load and e execution vulnerabilit e server to load and d Kerberos name-base nts if it did not strictly al domain compromise d Kerberos name-base
CVE-2017-74 CVE-2017-74 CVE-2020-17 CVE-2020-25	194 1 1494 1 17049 ! 5719 !	10.0 4 10.0 4 9.0 1 9.0 2	139 445 139 139 445 445	netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn	- Samba smbd 4.6.2 - Samba smbd	2022-02-27 2023-05-0 2022-02-27 2023-05-0 2023-04-27 2023-05-0 2022-03-02 2023-05-0 2023-04-27 2023-05-0	s Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. S Kerberos Security F 6 A flaw was found in authentication. The require a Kerberos S Kerberos Security F 6 A flaw was found in authentication. The	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 s client to upload a shared librar eature Bypass Vulnerability the way Samba, as an Active I Samba AD DC, could become PAC and always use the SIDs f eature Bypass Vulnerability the way Samba, as an Active I	y to a writable  o and 4.4.14 is y to a writable  Directory Doma confused about ound within. Tile  Directory Doma confused about ound about ound within about ound within about	share, and to vulnerable to share, and to share, and to share and to share result countries to the user a share result countries to the user a share and controllers to the user a share and the share	hen cause the oremote code then cause the first the cause the caus	e server to load and e execution vulnerabilit e server to load and d Kerberos name-base nts if it did not strictly al domain compromise d Kerberos name-base nts if it did not strictly
EVE-2017-74 EVE-2017-74 EVE-2020-17 EVE-2020-25 EVE-2020-25 EVE-2020-25	1494 11 1494 11 17049 ! 15719 !	10.0 4 10.0 4 9.0 1 9.0 2 9.0 4	139 445 139 139 445 445	netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn	- Samba smbd 4.6.2	2022-02-27 2023-05-0 2022-02-27 2023-05-0 2023-04-27 2023-05-0 2022-03-02 2023-05-0 2022-03-02 2023-05-0	S Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. S Kerberos Security F A flaw was found in authentication. The require a Kerberos E Kerberos Security F A flaw was found in authentication. The require a Kerberos Security F A flaw was found in authentication. The require a Kerberos Security F A flaw was found in authentication. The	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 s client to upload a shared librar eature Bypass Vulnerability  the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs feature Bypass Vulnerability the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs find the Way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs find the Way Samba maps domain	y to a writable o and 4.4.14 is y to a writable birectory Doma confused abou ound within. Ti birectory Doma confused abou ound within. Ti	vulnerable to share, and to share, and to ain Controller to the user a ne result countroller to the user a ne result countroller	hen cause the oremote code hen cause the r, implemented ticket represe lid include totar, implemented ticket represe lid include totare ticket represe lid include totare.	e server to load and e execution vulnerabilit e server to load and d Kerberos name-base nts if it did not strictly al domain compromise d Kerberos name-base nts if it did not strictly al domain compromise
EVE-2017-74 EVE-2017-74 EVE-2020-17 EVE-2020-25 EVE-2020-25 EVE-2020-25 EVE-2020-25	494 1 494 1 7049 9 5719 9 5719 9	10.0 1 10.0 2 9.0 1 9.0 2 9.0 2 8.5 1	139 445 139 139 445 445	netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn	- Samba smbd 4.6.2	2022-02-27 2023-05-0 2022-02-27 2023-05-0 2023-04-27 2023-05-0 2022-03-02 2023-05-0 2022-03-02 2023-05-0 2022-03-02 2023-05-0	S Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. S Kerberos Security F S A flaw was found in authentication. The require a Kerberos Security F S A flaw was found in authentication. The require a Kerberos Security F S A flaw was found in authentication. The require a Kerberos S A flaw was found in to cause possible p	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 s client to upload a shared librar eature Bypass Vulnerability the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs feature Bypass Vulnerability the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs for the way Samba and DC, could become PAC and always use the SIDs for the way Samba maps domain rivilege escalation.	y to a writable  D and 4.4.14 is y to a writable  Directory Doma confused about ound within. The Directory Doma confused about ound within. The users to local to	share, and the vulnerable to share, and the share, and the share, and the share, and the share are result countries to the share result countries the user an enersult countries. An automatic share share result countries are shared to share the share are shared to share the shared shared to share the shared shared shared to share the shared sha	hen cause the o remote code hen cause the r, implemented ticket represe ld include tota r, implemented ticket represe ld include tota thenticated att	e server to load and e execution vulnerabilit e server to load and d Kerberos name-base ints if it did not strictly al domain compromise d Kerberos name-base ints if it did not strictly al domain compromise tacker could use this fl
EVE-2017-74 EVE-2017-74 EVE-2020-17 EVE-2020-25 EVE-2020-25 EVE-2020-25 EVE-2020-25	494 1 494 1 7049 9 5719 9 5719 9	10.0 1 10.0 2 9.0 1 9.0 2 9.0 2 8.5 1	139 445 139 139 445 139 445	netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn	- Samba smbd 4.6.2	2022-02-27 2023-05-0 2022-02-27 2023-05-0 2023-04-27 2023-05-0 2022-03-02 2023-05-0 2022-03-02 2023-05-0 2022-03-02 2023-05-0	S Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. S Kerberos Security F A flaw was found in authentication. The require a Kerberos Security F A flaw was found in authentication. The require a Kerberos for the require a Kerberos for authentication. The require a Kerberos for a flaw was found in to cause possible p A flaw was found in to cause possible p	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 is client to upload a shared librar eature Bypass Vulnerability the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs feature Bypass Vulnerability the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs for the way Samba maps domain rivilege escalation.	y to a writable  D and 4.4.14 is y to a writable  Directory Doma confused about ound within. The Directory Doma confused about ound within. The users to local to	share, and the vulnerable to share, and the share, and the share, and the share, and the share are result countries to the share result countries the user an enersult countries. An automatic share share result countries are shared to share the share are shared to share the shared shared to share the shared shared shared to share the shared sha	hen cause the o remote code hen cause the r, implemented ticket represe ld include tota r, implemented ticket represe ld include tota thenticated att	e server to load and e execution vulnerabilit e server to load and d Kerberos name-base ints if it did not strictly al domain compromise d Kerberos name-base ints if it did not strictly al domain compromise tacker could use this fl
EVE-2017-74 EVE-2017-74 EVE-2020-17 EVE-2020-25 EVE-2020-25 EVE-2020-25 EVE-2020-25 EVE-2020-25	494 1 494 1 7049 9 5719 9 5717 3 5717 3	10.0 2 9.0 2 9.0 2 9.0 2 8.5 2	139 445 139 139 445 139 445	netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn	- Samba smbd 4.6.2	2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-03-02 2023-05-0 2022-03-02 2023-05-0 2022-03-02 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0	s Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. S Kerberos Security F A flaw was found in authentication. The require a Kerberos. Kerberos Security F A flaw was found in authentication. The require a Kerberos. The require a Kerberos in authentication. The require a Kerberos Security F A flaw was found in to cause possible p A flaw was found in to cause possible p	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 is client to upload a shared librar eature Bypass Vulnerability  the way Samba, as an Active I Samba AD DC, could become PAC and always use the SIDs feature Bypass Vulnerability  the way Samba, as an Active I Samba AD DC, could become PAC and always use the SIDs for the way Samba maps domain rivilege escalation.	y to a writable  o and 4.4.14 is y to a writable  Directory Doma confused about ound within. Til  Directory Doma confused about ound within. Til users to local to users to local to	share, and to vulnerable to share, and to share result could be share. The share result could be share to share result could be share. An autousers.	then cause the code then cause the c	e server to load and e execution vulnerabilit e server to load and d Kerberos name-base nts if it did not strictly al domain compromise d Kerberos name-base nts if it did not strictly al domain compromise tacker could use this fl
EVE-2017-74 EVE-2017-74 EVE-2020-17 EVE-2020-25 EVE-2020-25 EVE-2020-25 EVE-2020-25 EVE-2020-25	494 1 494 1 7049 9 5719 9 5717 3 5717 3	10.0 2 9.0 2 9.0 2 9.0 2 8.5 2	139 445 139 139 445 139 445	netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn	- Samba smbd 4.6.2	2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-03-02 2023-05-0 2022-03-02 2023-05-0 2022-03-02 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0	S Samba since versio allowing a malicious execute it. S Camba since versio allowing a malicious execute it. S Kerberos Security F S A flaw was found in authentication. The require a Kerberos S Camba	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 is client to upload a shared librar eature Bypass Vulnerability the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs feature Bypass Vulnerability the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs for the way Samba maps domain rivilege escalation.  the way Samba maps domain rivilege escalation.  all Samba versions before 4.10 P. This flaw allows a remote attreated.	y to a writable  2 and 4.4.14 is y to a writable  Directory Doma confused about ound within. The confused about ound within. The users to local the users to local the custom of the could be 2.17, before 4.3 cacker could to	wulnerable to share, and to vulnerable to share, and to controller to the user a ne result coursers. An autusers. An autusers. An autusers. An autusers. An autusers share use the Scause	hen cause the oremote code hen cause the representation of the code of the cod	e server to load and e execution vulnerabilit e server to load and d Kerberos name-base nts if it did not strictly al domain compromise d Kerberos name-base nts if it did not strictly al domain compromise tacker could use this fl tacker could use this fl the way it processed o consume excessive
CVE-2017-74  CVE-2017-74  CVE-2020-17  CVE-2020-25  CVE-2020-25  CVE-2020-25  CVE-2020-25  CVE-2020-25  CVE-2020-25  CVE-2020-25  CVE-2020-25  CVE-2020-16	1494 1494 1494 1494 1494 1494 1494 1494	9.0 2 9.0 9.0 9.0 8.5 2 8.5 7.8	139 445 139 139 445 445 139	netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn netbios	- Samba smbd 4.6.2	2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-03-02 2023-05-0 2022-03-02 2023-05-0 2022-03-02 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0	S Samba since versio allowing a malicious execute it. S Camba since versio allowing a malicious execute it. S Kerberos Security F A flaw was found in authentication. The require a Kerberos Security F A flaw was found in authentication. The require a Kerberos Security F A flaw was found in authentication. The require a Kerberos Security F A flaw was found in to cause possible p A flaw was found in to cause possible p A flaw was found in to cause possible p A flaw was found in to cause possible p A flaw was found in to cause possible p E A flaw was found in to cause possible p E A flaw was found in to cause possible p E A flaw was found in to cause possible p E A flaw was found in to cause possible p	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 is client to upload a shared librar eature Bypass Vulnerability the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs feature Bypass Vulnerability the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs for the way Samba maps domain rivilege escalation.  It was samba maps domain rivilege escalation.  all Samba versions before 4.10. This flaw allows a remote attlenial of service. This highest the	y to a writable  and 4.4.14 is y to a writable  Directory Doma confused about ound within. The birectory Doma confused about ound within. The users to local the users to local the confused about ound within. The confused about ound within the confu	wulnerable to share, and to vulnerable to share, and to share result could users. An autusers. An autusers. An autusers. An autusers share cause the Savulnerability in	hen cause the oremote code hen cause the representation of the code to the cod	e server to load and e execution vulnerabilit e server to load and d Kerberos name-base nts if it did not strictly al domain compromise d Kerberos name-base nts if it did not strictly al domain compromise tacker could use this fl tacker could use this fl the way it processed o consume excessive vailability.
EVE-2017-74 EVE-2017-74 EVE-2020-17 EVE-2020-25 EVE-2020-25 EVE-2020-25 EVE-2020-25 EVE-2020-25 EVE-2020-25	1494 1494 1494 1494 1494 1494 1494 1494	9.0 2 9.0 9.0 9.0 8.5 2 8.5 7.8	139 445 139 139 445 445 139 445	netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn netbios	- Samba smbd 4.6.2 - Samba smbd	2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-03-02 2023-05-0 2022-03-02 2023-05-0 2022-03-02 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0	S Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. S Kerberos Security F A flaw was found in authentication. The require a Kerberos. Kerberos Security F A flaw was found in authentication. The require a Kerberos of the foundation of the course of the foundation	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 is client to upload a shared librar client to upload a shared librar eature Bypass Vulnerability  the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs of the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs of the way Samba maps domain rivilege escalation.  the way Samba maps domain rivilege escalation.  all Samba versions before 4.10 P. This flaw allows a remote at lenial of service. This highest the all Samba versions before 4.10 Samba versions before	y to a writable  o and 4.4.14 is y to a writable  Directory Doma confused about ound within. Ti  Directory Doma confused about ound within. Ti  users to local usurers to local	vulnerable to share, and to vulnerable to share, and to share, and to share, and to share, and to share result could be share. An autousers. A	hen cause the oremote code then cause the first the cause the first the cause the first the cause the first the cause the fore 4.12.4 in and a server to see the cause the fore 4.12.4 in	e server to load and e execution vulnerabilit e server to load and d Kerberos name-base nts if it did not strictly al domain compromise d Kerberos name-base nts if it did not strictly al domain compromise tacker could use this fl tacker could use this fl the way it processed o consume excessive vailability. the way it processed
EVE-2017-74 EVE-2017-74 EVE-2020-17 EVE-2020-25 EVE-2020-25 EVE-2020-25 EVE-2020-25 EVE-2020-25 EVE-2020-25	1494 1494 1494 1494 1494 1494 1494 1494	9.0 2 9.0 9.0 9.0 8.5 2 8.5 7.8	139 445 139 139 445 445 139 445	netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn netbios	- Samba smbd 4.6.2	2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-03-02 2023-05-0 2022-03-02 2023-05-0 2022-03-02 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0	S Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. S Gamba since versio allowing a malicious execute it. S Kerberos Security F S A flaw was found in authentication. The require a Kerberos Security F S A flaw was found in authentication. The require a Kerberos 5 A flaw was found in to cause possible p S A flaw was found in to cause possible p S A flaw was found in NetBios over TCP/I use, resulting in a d S A flaw was found in NetBios over TCP/II use, resulting in a d S A flaw was found in NetBios over TCP/II use, resulting in a d S A flaw was found in NetBios over TCP/II use, resulting in a d	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 is client to upload a shared librar eature Bypass Vulnerability the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs feature Bypass Vulnerability the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs for the way Samba maps domain rivilege escalation.  It was samba maps domain rivilege escalation.  all Samba versions before 4.10. This flaw allows a remote attlenial of service. This highest the	y to a writable  2 and 4.4.14 is  3 to a writable  Directory Doma confused abou ound within. The  Directory Doma confused about ound	wulnerable to share, and to vulnerable to share, and to share result countries. An autiusers. An aut	hen cause the oremote code hen cause the r, implemented ticket represe lid include totary, implemented ticket represe ticket represe ticket represe the thenticated attributed totathenticated attributed to the thenticated attributed to the thentic	e server to load and e execution vulnerabilit e server to load and d Kerberos name-base nts if it did not strictly al domain compromise d Kerberos name-base nts if it did not strictly al domain compromise tacker could use this fl tacker could use this fl the way it processed o consume excessive vailability.
EVE-2017-74 EVE-2017-74 EVE-2020-17 EVE-2020-25 EVE-2020-25 EVE-2020-25 EVE-2020-26 EVE-2020-16 EVE-2020-16	1494 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	9.0 2 9.0 9.0 9.0 9.0 8.5 2 7.8 2 7.8	139 445 139 139 445 445 139 445	netbios ssn netbios netbios netbios ssn netbios ssn netbios ne	- Samba smbd 4.6.2 - Samba smbd	2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-03-02 2023-05-0 2022-03-02 2023-05-0 2022-03-02 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0	S Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. S Kerberos Security F S A flaw was found in authentication. The require a Kerberos Security F S A flaw was found in authentication. The require a Kerberos S A flaw was found in to cause possible p S A flaw was found in to cause possible p S A flaw was found in NetBios over TCP/I use, resulting in a d S A flaw was found in NetBios over TCP/I use, resulting in a d	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 s client to upload a shared librar eature Bypass Vulnerability  the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs feature Bypass Vulnerability  the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs freature Bypass Vulnerability  the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs f.  the way Samba maps domain rivilege escalation.  the way Samba maps domain rivilege escalation.  all Samba versions before 4.10  P. This flaw allows a remote attental of service. This highest lail Samba versions before 4.10  P. This flaw allows a remote attental Samba versions before 4.10  P. This flaw allows a remote attental samba versions before 4.10  P. This flaw allows a remote attental samba versions before 4.10  P. This flaw allows a remote attental samba versions before 4.10	ond 4.4.14 is y to a writable on and 4.4.14 is y to a writable or a writ	wulnerable to share, and to vulnerable to share, and the share, and th	hen cause the oremote code hen cause the representation of the code of the cod	e server to load and e execution vulnerabilit e server to load and d Kerberos name-base ints if it did not strictly al domain compromise d Kerberos name-base ints if it did not strictly al domain compromise tacker could use this fl tacker could use this fl the way it processed o consume excessive vailability.
EVE-2017-74 EVE-2017-74 EVE-2020-17 EVE-2020-25 EVE-2020-25 EVE-2020-25 EVE-2020-25 EVE-2020-16 EVE-2020-16	1494 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	9.0 9.0 9.0 9.0 9.0 8.5 9.7.8 4	139 445 139 139 445 445 139 445 139	netbios ssn netbios netbios netbios ssn netbios ssn netbios ne	- Samba smbd 4.6.2	2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-03-02 2023-05-0 2022-03-02 2023-05-0 2022-03-02 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0	S Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. S Kerberos Security F S A flaw was found in authentication. The require a Kerberos Security F S A flaw was found in authentication. The require a Kerberos S A flaw was found in to cause possible p S A flaw was found in to cause possible p S A flaw was found in NetBios over TCP/I use, resulting in a d S A flaw was found in NetBios over TCP/I use, resulting in a d	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 is client to upload a shared librar eature Bypass Vulnerability the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs feature Bypass Vulnerability the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs for the way Samba maps domain rivilege escalation. The way Samba maps domain rivilege escalation.  In the way Samba maps domain rivilege escalation.  In the way Samba waps domain rivilege escalation.	ond 4.4.14 is y to a writable on and 4.4.14 is y to a writable or a writ	wulnerable to share, and to vulnerable to share, and the share, and th	hen cause the oremote code hen cause the representation of the code of the cod	e server to load and e execution vulnerabilit e server to load and d Kerberos name-base ints if it did not strictly al domain compromise d Kerberos name-base ints if it did not strictly al domain compromise tacker could use this fl tacker could use this fl the way it processed o consume excessive vailability.
EVE-2017-74 EVE-2017-74 EVE-2020-17 EVE-2020-25 EVE-2020-25 EVE-2020-26 EVE-2020-26 EVE-2020-16 EVE-2020-16 EVE-2020-16	1494 1494 1494 1494 1494 1494 1494 1494	9.0 1 9.0 9.0 9.0 8.5 8.5 1 7.8 1 7.5 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	139 445 139 139 445 445 139 445 139 445	netbios ssn netbios ne	- Samba smbd 4.6.2	2022-02-27 2023-05-0 2023-04-27 2023-05-0 2023-04-27 2023-05-0 2023-04-27 2023-05-0 2022-03-02 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0	S Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. S Kerberos Security F S A flaw was found in authentication. The require a Kerberos is Kerberos Security F S A flaw was found in authentication. The require a Kerberos in authentication. The require a Kerberos is A flaw was found in to cause possible p S A flaw was found in NetBios over TCP/I use, resulting in A flaw was found in NetBios over TCP/I use, resulting in A flaw was found in SetBios over TCP/I use, resulting in a G Use-after-free vulne SMB1 request.	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 is client to upload a shared librar eature Bypass Vulnerability the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs feature Bypass Vulnerability the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs for the way Samba maps domain rivilege escalation. The way Samba maps domain rivilege escalation.  In the way Samba maps domain rivilege escalation.  In the way Samba waps domain rivilege escalation.	y to a writable  and 4.4.14 is y to a writable  Directory Doma confused about ound within. The  Directory Doma confused about ound within. The users to local the users to local the confused about acker could to reat from this to 0.17, before 4.3 acker could to reat from this to 0.17, before 4.3 acker could to reat from this to 0.17, before 4.3 acker could to reat from this to 0.3 acker could to reat from this to 0.3 acker could to 0.4 acker could to 0.5 acker could to 0.5 acker could to 0.6 acker could to 0.7 acker could to	wulnerable to share, and to vulnerable to share, and to share result coursers. An autusers. An autusers. An autusers. An autusers. An autusers share	hen cause the oremote code then cause the firm the cause the	e server to load and e execution vulnerabilit e server to load and d Kerberos name-base nts if it did not strictly al domain compromise d Kerberos name-base nts if it did not strictly al domain compromise tacker could use this fl tacker could use this fl tacker could use this fl the way it processed o consume excessive vailability. the way it processed o oronsume excessive vailability.
EVE-2017-74 EVE-2017-74 EVE-2020-17 EVE-2020-25 EVE-2020-25 EVE-2020-25 EVE-2020-26 EVE-2020-16 EVE-2020-16 EVE-2020-17 EVE-2017-14	1494 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	9.0 9.0 9.0 9.0 9.0 8.5 9.7.8 9.7.8 9.7.5	139 445 139 139 445 445 139 445 139 445	netbios ssn netbios ne	- Samba smbd 4.6.2	2022-02-27 2023-05-0 2023-04-27 2023-05-0 2022-03-02 2023-05-0 2022-03-02 2023-05-0 2022-03-02 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0	S Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. S Kerberos Security F S A flaw was found in authentication. The require a Kerberos Security F S A flaw was found in authentication. The require a Kerberos S A flaw was found in to cause possible p S A flaw was found in to cause possible p S A flaw was found in to cause possible p S A flaw was found in NetBios over TCP/I use, resulting in a d S A flaw was found in NetBios over TCP/I use, resulting in a d S Les-after-free vulne SMB1 request.	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 s client to upload a shared librar eature Bypass Vulnerability  the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs feature Bypass Vulnerability  the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs freature Bypass Vulnerability  the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs fithe way Samba maps domain rivilege escalation.  the way Samba maps domain rivilege escalation.  all Samba versions before 4.10 P. This flaw allows a remote attential of service. This highest th all Samba versions before 4.10 P. This flaw allows a remote attential of service. This highest the riability in Samba 4.x before 4.70 erability	y to a writable  2 and 4.4.14 is  3 to a writable  Directory Doma confused about ound within. The  directory Doma confused abo	share, and to vulnerable to share, and to vulnerable to share, and to share result countries to the share result countries. An autousers. An a	hen cause the oremote code hen cause the remote code hen cause the remote code hen cause the remote code include total remote code include total code include include total code include	e server to load and e execution vulnerabilit e server to load and d Kerberos name-base nts if it did not strictly al domain compromise d Kerberos name-base nts if it did not strictly al domain compromise tacker could use this fl tacker could use this fl the way it processed o consume excessive vailability. the way it processed o consume excessive vailability. bitrary code via a craft
EVE-2017-74 EVE-2017-74 EVE-2020-17 EVE-2020-25 EVE-2020-25 EVE-2020-25 EVE-2020-26 EVE-2020-16 EVE-2020-16 EVE-2020-16 EVE-2020-17 EVE-2017-14	1494 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	9.0 9.0 9.0 9.0 9.0 8.5 9.7.8 9.7.8 9.7.5	139 445 139 445 445 139 445 139 445 139 445 5060	netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn netbios	- Samba smbd 4.6.2	2022-02-27 2023-05-0 2023-04-27 2023-05-0 2022-03-02 2023-05-0 2022-03-02 2023-05-0 2022-03-02 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0	Samba since versio allowing a malicious execute it.  Samba since versio allowing a malicious execute it.  Kerberos Security F.  A flaw was found in authentication. The require a Kerberos.  A flaw was found in authentication. The require a Kerberos.  A flaw was found in authentication. The require a Kerberos.  A flaw was found in to cause possible p.  A flaw was found in to cause possible p.  A flaw was found in NetBios over TCP/I use, resulting in a d.  A flaw was found in NetBios over TCP/I use, resulting in a d.  Use-after-free vulne.  SMB1 request.  Use-after-free vulne.  SMB1 request.  Use-after-free vulne.  SMB1 request.	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 s client to upload a shared librar eature Bypass Vulnerability  the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs feature Bypass Vulnerability  the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs for the way Samba maps domain rivilege escalation.  the way Samba maps domain rivilege escalation.  all Samba versions before 4.10 P. This flaw allows a remote attalenial of service. This highest the all Samba versions before 4.10 P. This flaw allows a remote attalenial of service. This highest the could be service. This highest the service. This highest the could be service. This highest the service are service at the service and the service are service at the service and the service at th	y to a writable  2 and 4.4.14 is 2 to a writable  Directory Doma confused about ound within. The Directory Doma confused about ound within. The users to local the users to local the 2.17, before 4.1 acker could to reat from this the 2.3 allows remo 2.3 allows remo 3.4 allows remo 4.3 allows remo	wulnerable to share, and to vulnerable to share, and to share result countries. An autiliary and share result countries. An autiliary and share share result countries. An autiliary and share sha	hen cause the oremote code hen cause the representation of the code of the cause the representation of the code of the cause the representation of the code of the	e server to load and e execution vulnerabilit e server to load and d Kerberos name-base ints if it did not strictly al domain compromise d Kerberos name-base ints if it did not strictly al domain compromise tacker could use this fl tacker could use this fl the way it processed o consume excessive vailability. the way it processed o consume excessive vailability. bitrary code via a craft bitrary code via a craft
EVE-2017-74 EVE-2017-74 EVE-2020-17 EVE-2020-25 EVE-2020-25 EVE-2020-25 EVE-2020-26 EVE-2020-16 EVE-2020-16 EVE-2020-16 EVE-2020-17 EVE-2017-14	1494 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	9.0 9.0 9.0 9.0 9.0 8.5 9.7.8 9.7.8 9.7.5	139 445 139 445 445 139 445 139 445 139 445 5060	netbios ssn netbios ne	- Samba smbd 4.6.2 - Samba smbd	2022-02-27 2023-05-0 2023-04-27 2023-05-0 2022-03-02 2023-05-0 2022-03-02 2023-05-0 2022-03-02 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0	S Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. S Gamba since versio allowing a malicious execute it. S Kerberos Security F S A flaw was found in authentication. The require a Kerberos Security F S A flaw was found in authentication. The require a Kerberos S A flaw was found in to cause possible p S A flaw was found in to cause possible p S A flaw was found in to cause possible p S A flaw was found in NetBios over TCP/I use, resulting in a d S A flaw was found in NetBios over TCP/I use, resulting in a d S Use-after-free vulne SMB1 request. S Use-after-free vulne SMB1 request. S Use-after-free vulne SMB1 request.	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 is client to upload a shared librar eature Bypass Vulnerability  the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs for eature Bypass Vulnerability  the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs for the way Samba and DC, could become PAC and always use the SIDs for the way Samba maps domain rivilege escalation.  all Samba versions before 4.10 in all Samba versions before 4.	y to a writable  and 4.4.14 is y to a writable  Directory Doma confused about ound within. The  Directory Doma confused about ound the  Confused about ound within. The  Con	share, and to vulnerable to share, and to vulnerable to share, and to share result could an in Controller to the user and the users. An ault user	hen cause the oremote code hen cause the r, implemented ticket represe ild include total thenticated attributed to the thentic	e server to load and e execution vulnerabilit e server to load and d Kerberos name-base nts if it did not strictly al domain compromise d Kerberos name-base nts if it did not strictly al domain compromise tacker could use this fl tacker could use this fl tacker could use this fl the way it processed o consume excessive vailability. bitrary code via a craft bitrary code via a craft
EVE-2017-74 EVE-2017-74 EVE-2017-74 EVE-2020-15 EVE-2020-25 EVE-2020-25 EVE-2020-26 EVE-2020-16 EVE-2020-16 EVE-2020-16 EVE-2017-14 EVE-2017-14	1494 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	9.0 : 9.0 :	139 445 139 145 445 139 445 139 445 139 445 139 5060	netbios ssn netbios ne	- Samba smbd 4.6.2 - Samba smbd	2022-02-27 2023-05-0 2023-04-27 2023-05-0 2022-03-02 2023-05-0 2022-03-02 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0	S Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. S Kerberos Security F S A flaw was found in authentication. The require a Kerberos Security F S A flaw was found in authentication. The require a Kerberos Security F S A flaw was found in authentication. The require a Kerberos Security F S A flaw was found in to cause possible p S A flaw was found in to cause possible p S A flaw was found in NetBios over TCP/I use, resulting in a d S A flaw was found in NetBios over TCP/I use, resulting in a d S Use-after-free vulne SMB1 request. S MB1 request. S MB1 request. S MB1 request.	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 is client to upload a shared librar eature Bypass Vulnerability the way Samba, as an Active Eamba AD DC, could become PAC and always use the SIDs feature Bypass Vulnerability the way Samba, as an Active Eamba AD DC, could become PAC and always use the SIDs for the way Samba, as an Active Eamba AD DC, could become PAC and always use the SIDs for the way Samba maps domain rivilege escalation.  Ithe way Samba was a remote attention of the way Samba was a remote attention of	y to a writable  2 and 4.4.14 is y to a writable  Directory Doma confused about ound within. Til  Directory Doma confused about ound within. Til  users to local the users to local the confused about acker could to reat from this the confused about acker could to reat from this the confused about acker could to reat from this the confused acker could to reat from this the could be confused acker could to reat from this the confused acker confused a	share, and to vulnerable to share, and to vulnerable to share, and to sh	hen cause the oremote code hen cause the femore code hen cause femore code her c	e server to load and e execution vulnerabilit e server to load and d Kerberos name-base ints if it did not strictly al domain compromise d Kerberos name-base ints if it did not strictly al domain compromise tacker could use this fl tacker could use this fl tacker could use this fl the way it processed o consume excessive vailability. the way it processed o consume excessive vailability. bitrary code via a craft consume excessive vailability.
EVE-2017-74 EVE-2017-74 EVE-2017-74 EVE-2020-15 EVE-2020-25 EVE-2020-25 EVE-2020-26 EVE-2020-16 EVE-2020-16 EVE-2020-16 EVE-2017-14 EVE-2017-14	1494 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	9.0 9.0 9.0 9.0 9.0 8.5 9.7.8 9.7.8 9.7.5	139 445 139 139 445 445 139 445 139 445 139 445 139 445 139	netbios ssn netbios netbio	- Samba smbd 4.6.2 - Samba smbd	2022-02-27 2023-05-0 2023-04-27 2023-05-0 2022-03-02 2023-05-0 2022-03-02 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0	S Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. Kerberos Security F A flaw was found in authentication. The require a Kerberos. Kerberos Security F A flaw was found in authentication. The require a Kerberos. A flaw was found in authentication. The require a Kerberos. A flaw was found in to cause possible p A flaw was found in NetBios over TCP/I use, resulting in a d A flaw was found in NetBios over TCP/I use, resulting in a d A flaw was found in NetBios over TCP/I use, resulting in a d A flaw was found in NetBios over TCP/I use, resulting in a d A flaw was found in NetBios over TCP/I use, resulting in a d A flaw was found in NetBios over TCP/I use, resulting in a d A flaw was found in NetBios over TCP/I use, resulting in a d A flaw was found in NetBios over TCP/I use, resulting in a d A flaw was found in NetBios over TCP/I use, resulting in a d A flaw was found in NetBios over TCP/I use, resulting in a d A flaw was found in NetBios over TCP/I use, resulting in a d A flaw was found in NetBios over TCP/I use, resulting in a d A flaw was found in NetBios over TCP/I use, resulting in a d A flaw was found in NetBios over TCP/I use, resulting in a d A flaw was found in NetBios over TCP/I use, resulting in a d A flaw was found in NetBios over TCP/I use, resulting in a d A flaw was found in NetBios over TCP/I use, resulting in a d A flaw control over TCP/I use, resulting in a d A flaw control over TCP/I use, resulting in a d A flaw control over TCP/I use, resulting in a d A flaw control over TCP/I use, resulting in a d A flaw control over TCP/I use, resulting in a d A flaw control over TCP/I use, resulting in a d A flaw control over TCP/I use, resulting in a d A flaw control over TCP/I use, resulting in a d A flaw control over TCP/I use, resulting in a d A flaw control over TCP/I use, resulting in a d A flaw control over TCP/I use, resulting in a d A flaw control over TCP/I use, resulting in a d A flaw cont	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 is client to upload a shared librar ceature Bypass Vulnerability the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs of Feature Bypass Vulnerability the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs of the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs of the way Samba maps domain rivilege escalation.  all Samba versions before 4.10 in all Samba	y to a writable  2 and 4.4.14 is 2 to a writable  Directory Doma confused about ound within. The Directory Doma confused about ound within. The users to local the users to local the cacker could to reat from this the 2.3 allows remo 2.3 allows remo 2.4 allows remo 2.5 allows remo 2.6 allows remo 2.6 allows remo 2.7 allows remo 2.8 allows remo 3.9 allows remo 4.1 allows remo 4.2 allows remo 4.3 allows remo 4.3 allows remo 4.3 allows remo 4.4 allows remo 4.5 allows remo 4.6 allows remo 4.7 allows remo 4.8 allows remo 4.9 allows remo 4.0 a	wulnerable to share, and to vulnerable to share, and to share result could like the user a ne result could like the users. An autiliary share the Savulnerability in the share the Savulnerability in the attackers ofte attackers ofte attackers sterisk through characters is ection. This is the share the shar	hen cause the oremote code hen cause the firm that could be to the cause the firm that could be to the cause the firm that cated at the cause that cause the	e server to load and e execution vulnerabilit e server to load and d Kerberos name-base ints if it did not strictly al domain compromise d Kerberos name-base ints if it did not strictly al domain compromise tacker could use this fl tacker could use this fl tacker could use this fl the way it processed o consume excessive vailability. the way it processed o consume excessive vailability. bitrary code via a craft bitrary code via a craft bitrary code via a craft s. The func_odbc mode s, resulting in user- 15.2, 18.11.2, and 19.3 acks because it obtains
CVE-2017-74 CVE-2017-74 CVE-2020-17 CVE-2020-25 CVE-2020-25 CVE-2020-25 CVE-2020-25 CVE-2020-16 CVE-2020-26 CVE-2020-26	1494 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	9.0 : 9.0 :	139 445 139 139 445 445 139 445 139 445 139 445 139 445 139	netbios ssn netbios ne	- Samba smbd 4.6.2 - Samba smbd	2022-02-27 2023-05-0 2023-04-27 2023-05-0 2022-03-02 2023-05-0 2022-03-02 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0	S Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. S Kerberos Security F S A flaw was found in authentication. The require a Kerberos Security F S A flaw was found in authentication. The require a Kerberos Security F S A flaw was found in to cause possible p S A flaw was found in to cause possible p S A flaw was found in to cause possible p S A flaw was found in NetBios over TCP/I use, resulting in a d S Heisen S Wester free vulne SMB1 request. S MB1 request. S MB1 request. S MB2 request. S MB3 request. S MB3 request. S MB4 request. S MB6 request. S MB6 request. S MB7 request. S MB7 request. S MB7 request. S MB8 request. S MB8 request. S MB8 request. S MB8 request. S MB9 request.	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 is client to upload a shared librar eature Bypass Vulnerability the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs of Feature Bypass Vulnerability the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs of the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs of the way Samba maps domain rivilege escalation.  The way Samba maps domain rivilege escalation.  The way Samba maps domain rivilege escalation.  The way Samba was a remote atticential of service. This highest the entilege escalation.  The way Samba was a could be come of the was a remote atticential of service.  The way Samba was a could be come of the was a remote atticential of service.  The way Samba was a could be come of the was a remote atticential of the was a	y to a writable  2 and 4.4.14 is 2 to a writable  Directory Doma confused about ound within. Til  Directory Doma confused about ound within. Til  users to local the users to local the cacker could to reat from this value acker could to reat from	share, and the vulnerable to share, and the share result could be shared to share the share result could be shared to share the shared to share the shared to shared the shared to share the shared to shared the shared t	hen cause the oremote code hen cause the first code hence the first code henc	e server to load and e execution vulnerabilit e server to load and d Kerberos name-base ints if it did not strictly al domain compromise d Kerberos name-base ints if it did not strictly al domain compromise tacker could use this fl tacker could use this fl tacker could use this fl the way it processed to consume excessive vailability. the way it processed to consume excessive vailability. bitrary code via a craft consume excessive vailability. bitrary code via a craft
EVE-2017-74 EVE-2017-74 EVE-2017-74 EVE-2020-15 EVE-2020-25 EVE-2020-25 EVE-2020-26 EVE-2020-16 EVE-2020-16 EVE-2020-16 EVE-2017-14 EVE-2017-14	1494 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	9.0 : 9.0 :	139 445 139 139 445 445 139 445 139 445 139 445 139 445 139	netbios ssn netbios netbio	- Samba smbd 4.6.2 - Samba smbd	2022-02-27 2023-05-0 2023-04-27 2023-05-0 2022-03-02 2023-05-0 2022-03-02 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0	S Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. Kerberos Security F A flaw was found in authentication. The require a Kerberos. Kerberos Security F A flaw was found in authentication. The require a Kerberos of a flaw was found in to cause possible p A flaw was found in to cause possible p A flaw was found in NetBios over TCP/I use, resulting in a d A flaw was found in NetBios over TCP/I use, resulting in a d A flaw was found in NetBios over TCP/I use, resulting in a d A flaw was found in NetBios over TCP/I use, resulting in a d A flaw was found in NetBios over TCP/I use, resulting in a d A flaw was found in NetBios over TCP/I use, resulting in a d A flaw was found in NetBios over TCP/I use, resulting in a d A flaw was found in NetBios over TCP/I use, resulting in a d A flaw was found in NetBios over TCP/I use, resulting in a d A flaw was found in NetBios over TCP/I use, resulting in a d A flaw was found in the SMB1 request. C be-after-free vulne SMB1 request.	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 s client to upload a shared librar catter Bypass Vulnerability  the way Samba, as an Active I Samba AD DC, could become PAC and always use the SIDs feature Bypass Vulnerability  the way Samba, as an Active I Samba AD DC, could become PAC and always use the SIDs for the way Samba, as an Active I Samba AD DC, could become PAC and always use the SIDs for the way Samba maps domain rivilege escalation.  all Samba versions before 4.10 P. This flaw allows a remote attained of service. This highest the crability in Samba 4.x before 4.7 erability in Samba 4.x before 4.7 erability in Samba 4.x before 4.7 evered in Asterisk through 19.x a ladequate escaping functionality ing a broken SQL query or possuallows remote attackers to impures in a way that violates the kame must be obtained from the seet. Use of the unencrypted vered.	y to a writable  2) and 4.4.14 is 2) to a writable  2) and 4.4.14 is 3) to a writable  2) and 4.4.14 is 3) to a writable  2) confused about 2) confused abou	share, and to vulnerable to share, and to vulnerable to share, and to share result could an Controller to the user a ne result could users. An autousers. An autousers. An autousers. An autousers. An autousers. An autousers in the same the Savulnerability in the attackers of the attackers sterisk through characters is considered in the save with Orphotocol specific sterisk through the save with Orphotocol specific steriesk through the save with Orphotocol specific	hen cause the oremote code hen cause the remote code include total code include total thenticated atthenticated at the stopped in	e server to load and e execution vulnerabilit e server to load and d Kerberos name-base nts if it did not strictly al domain compromise d Kerberos name-base nts if it did not strictly al domain compromise tacker could use this fl tacker could use this fl tacker could use this fl the way it processed o consume excessive vailability. bitrary code via a craft bitrary code via a craft strictly is trace of the user color product of the color strictly strictly al domain compromise tacker could use this fl tacker could use
CVE-2017-74 CVE-2017-74 CVE-2020-17 CVE-2020-25 CVE-2020-25 CVE-2020-25 CVE-2020-25 CVE-2020-25	1494 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	9.0 : 9.0 :	139 445 139 139 445 445 139 445 139 445 139 445 139 445 139	netbios ssn netbios netbio	- Samba smbd 4.6.2 - Samba smbd	2022-02-27 2023-05-0 2023-04-27 2023-05-0 2022-03-02 2023-05-0 2022-03-02 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0	S Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. S Kerberos Security F S A flaw was found in authentication. The require a Kerberos is Kerberos Security F A A flaw was found in authentication. The require a Kerberos is A flaw was found in to cause possible p A flaw was found in to cause possible p A flaw was found in to cause possible p A flaw was found in NetBios over TCP/I use, resulting in A flaw was found in NetBios over TCP/I use, resulting in P found in NetBios over TCP/I use, resulting in a C use-after-free vulne SMB1 request. S Use-after-free vulne SMB1 request. An issue was discorprovides possibly in provided data creat and 16.8-cert14. S ervice-principal na KDC-REP service revrsion stored in 'tic and other attacks. N	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 is client to upload a shared librar eature Bypass Vulnerability  the way Samba, as an Active I Samba AD DC, could become PAC and always use the SIDs feature Bypass Vulnerability  the way Samba, as an Active I Samba AD DC, could become PAC and always use the SIDs feature Bypass Vulnerability  the way Samba, as an Active I Samba AD DC, could become PAC and always use the SIDs fithe way Samba maps domain rivilege escalation.  the way Samba maps domain rivilege escalation.  all Samba versions before 4.10 P. This flaw allows a remote attricental of service. This highest the lenial of service. This highest the rability in Samba 4.x before 4.70 erability in Samba 4.x before 4.70 e	y to a writable  2 and 4.4.14 is 2 to a writable  Directory Doma confused about ound within. The  Directory Doma confused about ound to reat from this v  C.3 allows remo C.4 allows remo C.5 allows remo C.5 allows remo C.5 allows remo C.6 allows remo C.7 allows remo C.8 allows remo C.9	share, and the vulnerable to share, and the share result countries the user and the share result countries. An authorized the share	hen cause the oremote code hen cause the r, implemented ticket represe lid include totary, implemented ticket represe lid include totary, implemented ticket represe the represe lid include totary in the represe that thenticated at the thenticated at the the represe the representation of the representation o	e server to load and e execution vulnerabilit e server to load and d Kerberos name-base nts if it did not strictly al domain compromise d Kerberos name-base nts if it did not strictly al domain compromise tacker could use this fl tacker could use this fl tacker could use this fl the way it processed o consume excessive vailability. bitrary code via a craft bitrary code via a craft strictly is trace of the user color product of the color strictly strictly al domain compromise tacker could use this fl tacker could use
CVE-2017-74 CVE-2017-74 CVE-2020-17 CVE-2020-25 CVE-2020-25 CVE-2020-25 CVE-2020-25 CVE-2020-16 CVE-2020-26 CVE-2020-26	494 1 1 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4	9.0 : 9.0 :	139 445 139 445 445 139 445 139 445 139 445 139 445 139 445	netbios ssn netbios ne	- Samba smbd 4.6.2 - Samba smbd	2022-02-27 2023-05-0 2023-04-27 2023-05-0 2023-04-27 2023-05-0 2023-04-27 2023-05-0 2022-03-02 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0	S Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. S Kerberos Security F S A flaw was found in authentication. The require a Kerberos Security F S A flaw was found in authentication. The require a Kerberos in authentication. The require a Kerberos S A flaw was found in to cause possible p S A flaw was found in to cause possible p S A flaw was found in to cause possible p S A flaw was found in NetBios over TCP/I use, resulting in a for A flaw was found in NetBios over TCP/I use, resulting in all S A flaw was found in S Les-after-free vulne SMB1 request. S Use-after-free vulne SMB1 request. S Use-after-free vulne SMB1 request. S Use-after-free vulne SMB1 request. S Les-after-free vulne SMB1 request.	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 s client to upload a shared librar eature Bypass Vulnerability  the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs feature Bypass Vulnerability  the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs fithe way Samba maps domain rivilege escalation.  the way Samba maps domain rivilege escalation.  all Samba versions before 4.10 P. This flaw allows a remote attenial of service. This highest the rail Samba versions before 4.10 P. This flaw allows a remote attenial of service. This highest the rability in Samba 4.x before 4.7 erability in Samba 4.x bef	ond 4.4.14 is y to a writable on and 4.4.14 is y to a writable or one of the property of a writable or one of the property of	wulnerable to share, and to vulnerable to share, and to vulnerable to share, and to share, and to share, and to share, and to share result countries to the user a ne result countries. An autusers. An	hen cause the oremote code hen cause the femore code hen cause for extra code hen cause for extra code hen code he code hen code he code hen code he code hen code he code hen code he code hen code hen code	e server to load and e execution vulnerabilit e server to load and d Kerberos name-base nts if it did not strictly al domain compromise d Kerberos name-base nts if it did not strictly al domain compromise tacker could use this fl tacker could use this fl tacker could use this fl the way it processed o consume excessive vailability. the way it processed o consume excessive vailability. bitrary code via a craft compressive stacker could use this fl the way it processed o consume excessive vailability. bitrary code via a craft bitrary code via a craft bitrary code via a craft compressive stacker could use consume excessive vailability. bitrary code via a craft consumer consum
CVE-2017-74 CVE-2017-74 CVE-2020-17 CVE-2020-25 CVE-2020-25 CVE-2020-25 CVE-2020-25 CVE-2020-16 CVE-2020-16 CVE-2017-14 CVE-2017-14 CVE-2017-14 CVE-2017-14 CVE-2017-14 CVE-2017-14	494 1 1 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4	9.0 : 9.0 :	139 445 139 445 445 139 445 139 445 139 445 139 445 445	netbios ssn netbios ne	- Samba smbd 4.6.2	2022-02-27 2023-05-0 2023-04-27 2023-05-0 2023-04-27 2023-05-0 2023-04-27 2023-05-0 2022-03-02 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0	Samba since versio allowing a malicious execute it.  Samba since versio allowing a malicious execute it.  Samba since versio allowing a malicious execute it.  Kerberos Security F  A flaw was found in authentication. The require a Kerberos is Kerberos Security F  A flaw was found in authentication. The require a Kerberos is A flaw was found in to cause possible p of A flaw was found in to cause possible p in to cause possible p in the composition of the composition	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 s client to upload a shared librar catter Bypass Vulnerability  the way Samba, as an Active I Samba AD DC, could become PAC and always use the SIDs feature Bypass Vulnerability  the way Samba, as an Active I Samba AD DC, could become PAC and always use the SIDs for the way Samba, as an Active I Samba AD DC, could become PAC and always use the SIDs for the way Samba maps domain rivilege escalation.  the way Samba maps domain rivilege escalation.  all Samba versions before 4.10 P. This flaw allows a remote attribute all Samba versions before 4.11 P. This flaw allows a remote attribute all of service. This highest the control of service. This highest the reability in Samba 4.x before 4.7 erability in Samba 4.x before 4.10 erability in Samba 4.x before 4.10 erability in Samba 4.x	y to a writable  2) and 4.4.14 is 2) to a writable  Directory Doma confused about ound within. The  Directory Doma confused ab	share, and to vulnerable to share, and to vulnerable to share, and to share result could are shared to share the Sarulnerability in the shared to share the Sarulnerability in the attackers of the attackers of the attackers of the attackers are considered in the shared	hen cause the oremote code hen cause the remote code include total code include total thenticated attributed attributed the code in code code code code code code code code	e server to load and e execution vulnerabilit e server to load and d Kerberos name-base nts if it did not strictly al domain compromise d Kerberos name-base nts if it did not strictly al domain compromise to the total compromise to the total compromise to the way it processed to consume excessive vailability. The way it processed to consume excessive the way it processed to consume excessive to consume excessive to consume excessive to consume exc
CVE-2017-74 CVE-2017-74 CVE-2020-17 CVE-2020-25 CVE-2020-25 CVE-2020-25 CVE-2020-25 CVE-2020-16 CVE-2020-16 CVE-2017-14 CVE-2017-14 CVE-2017-14 CVE-2017-14 CVE-2017-14 CVE-2017-14	494 1 1 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4	9.0 : 9.0 :	139 445 139 445 445 139 445 139 445 139 445 139 445 445	netbios ssn netbios	- Samba smbd 4.6.2	2022-02-27 2023-05-0 2023-04-27 2023-05-0 2023-04-27 2023-05-0 2023-04-27 2023-05-0 2022-03-02 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0	S Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. S Kerberos Security F S A flaw was found in authentication. The require a Kerberos Security F S A flaw was found in authentication. The require a Kerberos S A flaw was found in to cause possible p S A flaw was found in to cause possible p S A flaw was found in to cause possible p S A flaw was found in to cause possible p S A flaw was found in NetBios over TCP/I use, resulting in a d S A flaw was found in NetBios over TCP/I use, resulting in a d S L Seafter-free vulne SMB1 request. S Use-after-free vulne SMB1 request. S Use-after-free vulne SMB1 request. S Les-wice-principal na KDC-REP service reversion stored in tic and other attacks. No to other instances in the first periode in the service-principal na KDC-REP service in version stored in tic. S Heimdal before 7.4 service-principal na KDC-REP service in version stored in tic.	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 s client to upload a shared librar eature Bypass Vulnerability  If the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs of Feature Bypass Vulnerability  If the way Samba, as an Active E Samba AD DC, could become PAC and always use the SIDs of the way Samba maps domain rivilege escalation.  If the way Samba was remote attential of service. This highest the remail of service. This highest the reability in Samba 4.x before 4.7 erability in Samba 4.x before 4.7 erab	ond 4.4.14 is y to a writable on and 4.4.14 is y to a writable or a writ	wulnerable to share, and to vulnerable to share, and to vulnerable to share, and to share result countries. An autility of the share share result countries, and the share	hen cause the oremote code hen cause the femore code hen code hen code hen cause the femore cause the femore code hen cause the ca	e server to load and e execution vulnerabilit e server to load and d Kerberos name-base nts if it did not strictly al domain compromise d Kerberos name-base nts if it did not strictly al domain compromise tacker could use this fl the way it processed o consume excessive vailability. the way it processed o consume excessive vailability. bitrary code via a craft consume server se
CVE-2017-74 CVE-2017-74 CVE-2020-17 CVE-2020-25 CVE-2020-25 CVE-2020-25 CVE-2020-25 CVE-2020-16 CVE-2020-16 CVE-2017-14 CVE-2017-14 CVE-2017-14 CVE-2017-14 CVE-2017-14 CVE-2017-14	494 1 1 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4	9.0 : 9.0 :	139 445 139 445 445 139 445 139 445 139 445 139 445 445	netbios ssn netbios	- Samba smbd 4.6.2	2022-02-27 2023-05-0 2023-04-27 2023-05-0 2023-04-27 2023-05-0 2023-04-27 2023-05-0 2022-03-02 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0	S Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. Kerberos Security F A flaw was found in authentication. The require a Kerberos. Kerberos Security F A flaw was found in authentication. The require a Kerberos. A flaw was found in authentication. The require a Kerberos. A flaw was found in to cause possible p A flaw was found in NetBios over TCP/I use, resulting in a d S A flaw was found in NetBios over TCP/I use, resulting in A d S A flaw was found in NetBios over TCP/I use, resul	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 s client to upload a shared librar catter Bypass Vulnerability  the way Samba, as an Active I Samba AD DC, could become PAC and always use the SIDs feature Bypass Vulnerability  the way Samba, as an Active I Samba AD DC, could become PAC and always use the SIDs for the way Samba, as an Active I Samba AD DC, could become PAC and always use the SIDs for the way Samba maps domain rivilege escalation.  the way Samba maps domain rivilege escalation.  all Samba versions before 4.10 P. This flaw allows a remote attribute all Samba versions before 4.11 P. This flaw allows a remote attribute all of service. This highest the control of service. This highest the reability in Samba 4.x before 4.7 erability in Samba 4.x before 4.10 erability in Samba 4.x before 4.10 erability in Samba 4.x	y to a writable  2 and 4.4.14 is 2 to a writable  Directory Doma confused about ound within. Ti  Directory Doma confused about ound within. Ti  users to local to users to local to acker could to reat from this v acker coul	share, and to vulnerable to share, and to vulnerable to share, and to controller to the user a ne result could users. An autilisers. An autilisers	hen cause the oremote code hen cause the firm of the code hen cause the code hen cause the code hen	e server to load and e execution vulnerabilit e server to load and d Kerberos name-base ints if it did not strictly al domain compromise d Kerberos name-base ints if it did not strictly al domain compromise tacker could use this fi the way it processed o consume excessive vailability. the way it processed o consume excessive vailability. bitrary code via a craft 5_extract_ticket() the stead of the unencryp sful server impersonat dal code; it does not a acks because it obtains 5_extract_ticket() the stead of the unencryp sful server impersonat restead of the unencryp sful server impersonat cacks because it obtains 5_extract_ticket() the stead of the unencryp sful server impersonat
EVE-2017-74 EVE-2017-74 EVE-2020-17 EVE-2020-25 EVE-2020-25 EVE-2020-25 EVE-2020-26 EVE-2020-16 EVE-2020-16 EVE-2017-14 EVE-2017-14 EVE-2017-14	494 1 1 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4	9.0 : 9.0 :	139 445 139 445 445 139 445 139 445 139 445 139 445 445	netbios ssn netbios	- Samba smbd 4.6.2	2022-02-27 2023-05-0 2023-04-27 2023-05-0 2023-04-27 2023-05-0 2023-04-27 2023-05-0 2022-03-02 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0	S Samba since versio allowing a malicious execute it.  S Samba since versio allowing a malicious execute it.  S Samba since versio allowing a malicious execute it.  Kerberos Security F  A flaw was found in authentication. The require a Kerberos.  A flaw was found in authentication. The require a Kerberos.  A flaw was found in to cause possible p for a kerberos.  A flaw was found in to cause possible p in ketBios over TCP/I use, resulting in a d in the state of	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 is client to upload a shared librar call the state of the shared librar feature Bypass Vulnerability of the way Samba, as an Active I Samba AD DC, could become PAC and always use the SIDs of Feature Bypass Vulnerability of the way Samba, as an Active I Samba AD DC, could become PAC and always use the SIDs of the way Samba, as an Active I Samba AD DC, could become PAC and always use the SIDs of the way Samba maps domain rivilege escalation.  It was samba maps domain rivilege escalation.  It was Samba maps domain rivilege escalation.  It was Samba was remote attrivilege escalation.  It was samba was a remote attrivilege escalation.  It was a remote attrivilege the samble was a remote attrivilege escalation.  It was a remote attrivilege the samble was a remote attrivilege escalation.  It was a remote attrivilege the samble was a remote attrivilege escalation.  It was a remote attrivilege the samble was a remote attrivilege escalation.  It was a remote attrivilege the samble was a remote attrivilege escalation.  It was a remote attrivilege the samble was a remote attrivilege escalation.  It was a remote attrivilege the samble was a remote attrivilege escalation.	y to a writable  2 and 4.4.14 is  3 to a writable  Directory Doma confused abou ound within. The  Directory Doma confused about ound within. The  Directory Doma confused about ound the form this to ound Certified As of for backslash sibly a SQL injuit ound Ce	share, and to vulnerable to share, and to vulnerable to share, and to share result countries are result countries. An autousers.	hen cause the oremote code hen cause the remote cause the remote code hen cause the remote code	e server to load and e execution vulnerabilit e server to load and d Kerberos name-base ints if it did not strictly al domain compromise d Kerberos name-base ints if it did not strictly al domain compromise tacker could use this fi the way it processed o consume excessive vailability. the way it processed o consume excessive vailability. bitrary code via a craft 5_extract_ticket() the stead of the unencryp sful server impersonat dal code; it does not a acks because it obtains 5_extract_ticket() the stead of the unencryp sful server impersonat restead of the unencryp sful server impersonat cacks because it obtains 5_extract_ticket() the stead of the unencryp sful server impersonat
EVE-2017-74 EVE-2017-74 EVE-2020-17 EVE-2020-25 EVE-2020-25 EVE-2020-25 EVE-2020-26 EVE-2020-16 EVE-2020-16 EVE-2017-14 EVE-2017-14 EVE-2017-14	494 1 1 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4	10.0 2 2 3 9.0 2 3 9.0 2 4 9.0	139 445 139 145 445 139 445 139 445 139 445 139 445 139 445	netbios ssn netbios sn netbios ssn netbios netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn netbios ssn netbios net	- Samba smbd 4.6.2	2022-02-27 2023-05-0 2023-04-27 2023-05-0 2023-04-27 2023-05-0 2023-04-27 2023-05-0 2022-03-02 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0 2022-02-27 2023-05-0	S Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. S Samba since versio allowing a malicious execute it. Kerberos Security F A flaw was found in authentication. The require a Kerberos. Kerberos Security F A flaw was found in authentication. The require a Kerberos. A flaw was found in to cause possible p f A flaw was found in to cause possible p in to cause possible p in the cause possible p in A flaw was found in NetBios over TCP/I use, resulting in a d in the cause found in the cause possible p in A flaw was found in NetBios over TCP/I use, resulting in a d in the cause found in NetBios over TCP/I use, resulting in a d in the cause found in NetBios over TCP/I use, resulting in a d in the cause found in NetBios over TCP/I use, resulting in a d in	s client to upload a shared librar on 3.5.0 and before 4.6.4, 4.5.10 s client to upload a shared librar catter Bypass Vulnerability  the way Samba, as an Active I Samba AD DC, could become PAC and always use the SIDs feature Bypass Vulnerability  the way Samba, as an Active I Samba AD DC, could become PAC and always use the SIDs for the way Samba and DC, could become PAC and always use the SIDs for the way Samba maps domain rivilege escalation.  the way Samba maps domain rivilege escalation.  all Samba versions before 4.10 P. This flaw allows a remote atthe lenial of service. This highest the lall Samba versions before 4.11 P. This flaw allows a remote atthe lenial of service. This highest the rability in Samba 4.x before 4.7 erability in Samba	ond 4.4.14 is y to a writable on and 4.4.14 is y to a writable on and 4.4.14 is y to a writable on a	share, and to vulnerable to share, and to vulnerable to share, and to share and to share and to share and to share a share result could users. An autility of the share and to share a sha	hen cause the oremote code hen cause the oremote code hen cause the remote code he remote code hen cause the remote code her code h	e server to load and e execution vulnerabilit e server to load and d Kerberos name-base ints if it did not strictly al domain compromise d Kerberos name-base ints if it did not strictly al domain compromise d Kerberos name-base ints if it did not strictly al domain compromise tacker could use this fi tacker could use this fi tacker could use this fi the way it processed o consume excessive vailability. the way it processed o consume excessive vailability. bitrary code via a craft

CVE-2018-10858	6.5	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A heap-buffer overflow was found in the way samba clients processed extra long filename in a directory listing. A malicious samba server could use this flaw to cause arbitrary code execution on a samba client. Samba versions before 4.6.16, 4.7.9 and 4.8.4 are vulnerable.
CVE-2020-25718	6.5	139	netbios- ssn	Samba smbd 4.6.2	2022-03-02 2023-05-06	A flaw was found in the way samba, as an Active Directory Domain Controller, is able to support an RODC (read-only domain controller). This would allow an RODC to print administrator tickets.
CVE-2020-25722	6.5	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	Multiple flaws were found in the way samba AD DC implemented access and conformance checking of stored data.  An attacker could use this flaw to cause total domain compromise.
CVE-2021-3738	6.5	139	netbios- ssn	Samba smbd 4.6.2	2022-03-13 2023-05-06	In DCE/RPC it is possible to share the handles (cookies for resource state) between multiple connections via a mechanism called 'association groups'. These handles can reference connections to our sam.ldb database. However while the database was correctly shared, the user credentials state was only pointed at, and when one connection within that association group ended, the database would be left pointing at an invalid 'struct session_info'. The most likely outcome here is a crash, but it is possible that the use-after-free could instead allow different user state to be pointed at and this might allow more privileged access.
CVE-2018-1057	6.5	445	netbios- ssn	Samba smbd 4.6.2	2023-04-27 2023-05-06	On a Samba 4 AD DC the LDAP server in all versions of Samba from 4.0.0 onwards incorrectly validates permissions to modify passwords over LDAP allowing authenticated users to change any other users' passwords, including administrative users and privileged service accounts (eg Domain Controllers).
CVE-2018-10858	6.5	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A heap-buffer overflow was found in the way samba clients processed extra long filename in a directory listing. A malicious samba server could use this flaw to cause arbitrary code execution on a samba client. Samba versions before 4.6.16, 4.7.9 and 4.8.4 are vulnerable.
CVE-2020-25718	6.5	445	netbios- ssn	Samba smbd 4.6.2	2022-03-02 2023-05-06	A flaw was found in the way samba, as an Active Directory Domain Controller, is able to support an RODC (read-only domain controller). This would allow an RODC to print administrator tickets.
CVE-2020-25722	6.5	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	Multiple flaws were found in the way samba AD DC implemented access and conformance checking of stored data.  An attacker could use this flaw to cause total domain compromise.
CVE-2021-3738	6.5	445	netbios- ssn	Samba smbd 4.6.2	2022-03-13 2023-05-06	In DCE/RPC it is possible to share the handles (cookies for resource state) between multiple connections via a mechanism called 'association groups'. These handles can reference connections to our sam.ldb database. However while the database was correctly shared, the user credentials state was only pointed at, and when one connection within that association group ended, the database would be left pointing at an invalid 'struct session_info'. The most likely outcome here is a crash, but it is possible that the use-after-free could instead allow different user state to be pointed at and this might allow more privileged access.
CVE-2019-14870	6.4	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	All Samba versions 4.x.x before 4.9.17, 4.10.x before 4.10.11 and 4.11.x before 4.11.3 have an issue, where the S4U (MS-SFU) Kerberos delegation model includes a feature allowing for a subset of clients to be opted out of constrained delegation in any way, either S4U2Self or regular Kerberos authentication, by forcing all tickets for these clients to be non-forwardable. In AD this is implemented by a user attribute delegation_not_allowed (aka not-delegated), which translates to disallow-forwardable. However the Samba AD DC does not do that for S4U2Self and does set the forwardable flag even if the impersonated client has the not-delegated flag set.
CVE-2019-14870	6.4	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	All Samba versions 4.x.x before 4.9.17, 4.10.x before 4.10.11 and 4.11.x before 4.11.3 have an issue, where the S4U (MS-SFU) Kerberos delegation model includes a feature allowing for a subset of clients to be opted out of constrained delegation in any way, either S4U2Self or regular Kerberos authentication, by forcing all tickets for these clients to be non-forwardable. In AD this is implemented by a user attribute delegation not allowed (aka not-delegated), which translates to disallow-forwardable. However the Samba AD DC does not do that for S4U2Self and does set the forwardable flag even if the impersonated client has the not-delegated flag set.
CVE-2017-12150	5.8	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	It was found that samba before 4.4.16, 4.5.x before 4.5.14, and 4.6.x before 4.6.8 did not enforce "SMB signing" when certain configuration options were enabled. A remote attacker could launch a man-in-the-middle attack and retrieve information in plain-text.
CVE-2017-12151	5.8	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in the way samba client before samba 4.4.16, samba 4.5.14 and samba 4.6.8 used encryption with the max protocol set as SMB3. The connection could lose the requirement for signing and encrypting to any DFS redirects, allowing an attacker to read or after the contents of the connection via a man-in-the-middle attack.
CVE-2017-12150	5.8	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	It was found that samba before 4.4.16, 4.5.x before 4.5.14, and 4.6.x before 4.6.8 did not enforce "SMB signing" when certain configuration options were enabled. A remote attacker could launch a man-in-the-middle attack and retrieve information in plain-text.
CVE-2017-12151	5.8	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in the way samba client before samba 4.4.16, samba 4.5.14 and samba 4.6.8 used encryption with the max protocol set as SMB3. The connection could lose the requirement for signing and encrypting to any DFS redirects, allowing an attacker to read or alter the contents of the connection via a man-in-the-middle attack.
CVE-2019-14902	5.5	139	netbios- ssn	Samba smbd 4.6.2	2023-04-27 2023-05-06	There is an issue in all samba 4.11.x versions before 4.11.5, all samba 4.10.x versions before 4.10.12 and all samba 4.9.x versions before 4.9.18, where the removal of the right to create or modify a subtree would not automatically be taken away on all domain controllers.
CVE-2019-3880	5.5	139	netbios- ssn	Samba smbd 4.6.2	2023-04-27 2023-05-06	A flaw was found in the way samba implemented an RPC endpoint emulating the Windows registry service API. An unprivileged attacker could use this flaw to create a new registry hive file anywhere they have unix permissions which could lead to creation of a new file in the Samba share. Versions before 4.8.11, 4.9.6 and 4.10.2 are vulnerable.
CVE-2019-14902	5.5	445	netbios- ssn	Samba smbd 4.6.2	2023-04-27 2023-05-06	There is an issue in all samba 4.11.x versions before 4.11.5, all samba 4.10.x versions before 4.10.12 and all samba 4.9.x versions before 4.9.18, where the removal of the right to create or modify a subtree would not automatically be taken away on all domain controllers.
CVE-2019-3880	5.5	445	netbios- ssn	Samba smbd 4.6.2	2023-04-27 2023-05-06	A flaw was found in the way samba implemented an RPC endpoint emulating the Windows registry service API. An unprivileged attacker could use this flaw to create a new registry hive file anywhere they have unix permissions which could lead to creation of a new file in the Samba share. Versions before 4.8.11, 4.9.6 and 4.10.2 are vulnerable.
CVE-2017-15275	5.0	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	Samba before 4.7.3 might allow remote attackers to obtain sensitive information by leveraging failure of the server to clear allocated heap memory.
CVE-2020-10704	5.0	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found when using samba as an Active Directory Domain Controller. Due to the way samba handles certain requests as an Active Directory Domain Controller LDAP server, an unauthorized user can cause a stack overflow leading to a denial of service. The highest threat from this vulnerability is to system availability. This issue affects all samba versions before 4.10.15, before 4.11.8 and before 4.12.2.
CVE-2020-27840	5.0	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in samba. Spaces used in a string around a domain name (DN), while supposed to be ignored, can cause invalid DN strings with spaces to instead write a zero-byte into out-of-bounds memory, resulting in a crash. The highest threat from this vulnerability is to system availability.
CVE-2021-20277	5.0	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in Samba's libldb. Multiple, consecutive leading spaces in an LDAP attribute can lead to an out-of-bounds memory write, leading to a crash of the LDAP server process handling the request. The highest threat from this vulnerability is to system availability.
CVE-2017-15275	5.0	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	Samba before 4.7.3 might allow remote attackers to obtain sensitive information by leveraging failure of the server to clear allocated heap memory.
CVE-2020-10704	5.0	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found when using samba as an Active Directory Domain Controller. Due to the way samba handles certain requests as an Active Directory Domain Controller LDAP server, an unauthorized user can cause a stack overflow leading to a denial of service. The highest threat from this vulnerability is to system availability. This issue affects all samba versions before 4.10.15, before 4.11.8 and before 4.12.2.
CVE-2020-27840	5.0	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in samba. Spaces used in a string around a domain name (DN), while supposed to be ignored, can cause invalid DN strings with spaces to instead write a zero-byte into out-of-bounds memory, resulting in a crash. The highest threat from this vulnerability is to system availability.
CVE-2021-20277	5.0	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in Samba's libldb. Multiple, consecutive leading spaces in an LDAP attribute can lead to an out-of- bounds memory write, leading to a crash of the LDAP server process handling the request. The highest threat from this vulnerability is to system availability.
CVE-2021-26712	5.0	5060	sip- proxy	Asterisk PBX 16.12.0	2023-04-27 2023-05-06	Incorrect access controls in res_srtp.c in Sangoma Asterisk 13.38.1, 16.16.0, 17.9.1, and 18.2.0 and Certified Asterisk 16.8-certS allow a remote unauthenticated attacker to prematurely terminate secure calls by replaying SRTP packets.
CVE-2021-26717	5.0	5060		Asterisk PBX 16.12.0	2023-04-27 2023-05-06	An issue was discovered in Sangoma Asterisk 16.x before 16.16.1, 17.x before 17.9.2, and 18.x before 18.2.1 and Certified Asterisk before 16.8-cert6. When re-negotiating for T.38, if the initial remote response was delayed just enough, Asterisk would send both audio and T.38 in the SDP. If this happened, and the remote responded with a
						declined T.38 stream, then Asterisk would crash.

CVE-2021-3255	5.0	5060		Asterisk PBX 16.12.0	2023-04-27 2023-05-06	An issue was discovered in Sangoma Asterisk 13.x before 13.38.3, 16.x before 16.19.1, 17.x before 17.9.4, and 18.x before 18.5.1, and Certified Asterisk before 16.8-cert10. If the IAX2 channel driver receives a packet that contains an unsupported media format, a crash can occur.
CVE-2019-1483	4.9	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in Samba, all versions starting samba 4.5.0 before samba 4.9.15, samba 4.10.10, samba 4.11.2, in the way it handles a user password change or a new password for a samba user. The Samba Active Directory Domain Controller can be configured to use a custom script to check for password complexity. This configuration can fail to verify password complexity when non-ASCII characters are used in the password, which could lead to weak passwords being set for samba users, making it vulnerable to dictionary attacks.
CVE-2021-2025	4.9	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in samba. The Samba smbd file server must map Windows group identities (SIDs) into unix group ids (gids). The code that performs this had a flaw that could allow it to read data beyond the end of the array in the case where a negative cache entry had been added to the mapping cache. This could cause the calling code to return those values into the process token that stores the group membership for a user. The highest threat from this vulnerability is to data confidentiality and integrity.
CVE-2019-1483	3 4.9	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in Samba, all versions starting samba 4.5.0 before samba 4.9.15, samba 4.10.10, samba 4.11.2, in the way it handles a user password change or a new password for a samba user. The Samba Active Directory Domain Controller can be configured to use a custom script to check for password complexity. This configuration can fail to verify password complexity when non-ASCII characters are used in the password, which could lead to weak passwords being set for samba users, making it vulnerable to dictionary attacks.
CVE-2021-2025	4.9	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in samba. The Samba smbd file server must map Windows group identities (SIDs) into unix group ids (gids). The code that performs this had a flaw that could allow it to read data beyond the end of the array in the case where a negative cache entry had been added to the mapping cache. This could cause the calling code to return those values into the process token that stores the group membership for a user. The highest threat from this vulnerability is to data confidentiality and integrity.
CVE-2017-1216	4.8	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	An information leak flaw was found in the way SMB1 protocol was implemented by Samba before 4.4.16, 4.5.x before 4.5.14, and 4.6.x before 4.6.8. A malicious client could use this flaw to dump server memory contents to a file on the samba share or to a shared printer, though the exact area of server memory cannot be controlled by the attacker.
CVE-2017-1216	4.8	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	An information leak flaw was found in the way SMB1 protocol was implemented by Samba before 4.4.16, 4.5.x before 4.5.14, and 4.6.x before 4.6.8. A malicious client could use this flaw to dump server memory contents to a file on the samba share or to a shared printer, though the exact area of server memory cannot be controlled by the attacker.
CVE-2016-2124	4.3	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in the way samba implemented SMB1 authentication. An attacker could use this flaw to retrieve the plaintext password sent over the wire even if Kerberos authentication was required.
CVE-2016-2124	4.3	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in the way samba implemented SMB1 authentication. An attacker could use this flaw to retrieve the plaintext password sent over the wire even if Kerberos authentication was required.
CVE-2020-3577	4.3	5060	sip-	Asterisk PBX 16.12.0	2023-04-27 2023-05-06	A buffer overflow in res_pjsip_diversion.c in Sangoma Asterisk versions 13.38.1, 16.15.1, 17.9.1, and 18.1.1 allows remote attacker to crash Asterisk by deliberately misusing SIP 181 responses.
CVE-2021-2690	4.3	5060	sip-	Asterisk PBX 16.12.0	2023-04-27 2023-05-06	An issue was discovered in res_pisip_session.c in Digium Asterisk through 13.38.1; 14.x, 15.x, and 16.x through 16.16.0; 17.x through 17.9.1; and 18.x through 18.2.0, and Certified Asterisk through 16.8-cert5. An SDP negotiation vulnerability in PJSIP allows a remote server to potentially crash Asterisk by sending specific SIP responses that cause an SDP negotiation failure.
CVE-2018-1091	4.0	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	The Samba Active Directory LDAP server was vulnerable to an information disclosure flaw because of missing access control checks. An authenticated attacker could use this flaw to extract confidential attribute values using LDAP search expressions. Samba versions before 4.6.16, 4.7.9 and 4.8.4 are vulnerable.
CVE-2018-14629	4.0	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A denial of service vulnerability was discovered in Samba's LDAP server before versions 4.7.12, 4.8.7, and 4.9.3. A CNAME loop could lead to infinite recursion in the server. An unprivileged local attacker could create such an entry, leading to denial of service.
CVE-2018-1684	4.0	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	Samba from version 4.3.0 and before versions 4.7.12, 4.8.7 and 4.9.3 are vulnerable to a denial of service. When configured to accept smart-card authentication, Samba's KDC will call talloc_free() twice on the same memory if the principal in a validly signed certificate does not match the principal in the AS-REQ. This is only possible after authentication with a trusted certificate. talloc is robust against further corruption from a double-free with talloc_free() and directly calls abort(), terminating the KDC process.
CVE-2018-1685	4.0	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	Samba from version 4.0.0 and before versions 4.7.12, 4.8.7, 4.9.3 is vulnerable to a denial of service. During the processing of an LDAP search before Samba's AD DC returns the LDAP entries to the client, the entries are cached in a single memory object with a maximum size of 256MB. When this size is reached, the Samba process providing the LDAP service will follow the NULL pointer, terminating the process. There is no further vulnerability associated with this issue, merely a denial of service.
CVE-2019-1484	4.0	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in samba 4.0.0 before samba 4.9.15 and samba 4.10.x before 4.10.10. An attacker can crash AD DC LDAP server via dirsync resulting in denial of service. Privilege escalation is not possible with this issue.
CVE-2020-1073	4.0	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A NULL pointer dereference, or possible use-after-free flaw was found in Samba AD LDAP server in versions before 4.10.17, before 4.11.11 and before 4.12.4. Although some versions of Samba shipped with Red Hat Enterprise Linux do not support Samba in AD mode, the affected code is shipped with the libidb package. This flaw allows an authenticated user to possibly trigger a use-after-free or NULL pointer dereference. The highest threat from this vulnerability is to system availability.
CVE-2020-1076	4.0	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A use-after-free flaw was found in all samba LDAP server versions before 4.10.17, before 4.11.11, before 4.12.4 used in a AC DC configuration. A Samba LDAP user could use this flaw to crash samba.
CVE-2020-1431	4.0	139		Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in the way samba handled file and directory permissions. An authenticated user could use this flaw to gain access to certain file and directory information which otherwise would be unavailable to the attacker.
CVE-2020-1438	4.0	139	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in samba's DNS server. An authenticated user could use this flaw to the RPC server to crash. This RPC server, which also serves protocols other than dnsserver, will be restarted after a short delay, but it is easy for an authenticated non administrative attacker to crash it again as soon as it returns. The Samba DNS server itself will continue to operate, but many RPC services will not.
CVE-2018-1091	4.0	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	The Samba Active Directory LDAP server was vulnerable to an information disclosure flaw because of missing access control checks. An authenticated attacker could use this flaw to extract confidential attribute values using LDAP search expressions. Samba versions before 4.6.16, 4.7.9 and 4.8.4 are vulnerable.
CVE-2018-14629	4.0	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A denial of service vulnerability was discovered in Samba's LDAP server before versions 4.7.12, 4.8.7, and 4.9.3. A CNAME loop could lead to infinite recursion in the server. An unprivileged local attacker could create such an entry, leading to denial of service.
CVE-2018-1684	4.0	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	Samba from version 4.3.0 and before versions 4.7.12, 4.8.7 and 4.9.3 are vulnerable to a denial of service. When configured to accept smart-card authentication, Samba's KDC will call talloc_free() twice on the same memory if the principal in a validly signed certificate does not match the principal in the AS-REQ. This is only possible after authentication with a trusted certificate. talloc is robust against further corruption from a double-free with talloc_free() and directly calls abort(), terminating the KDC process.
CVE-2018-1685	4.0	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	Samba from version 4.0.0 and before versions 4.7.12, 4.8.7, 4.9.3 is vulnerable to a denial of service. During the processing of an LDAP search before Samba's AD DC returns the LDAP entries to the client, the entries are cached in a single memory object with a maximum size of 256MB. When this size is reached, the Samba process providing the LDAP service will follow the NULL pointer, terminating the process. There is no further vulnerability associated with this issue, merely a denial of service.
CVE-2019-1484	4.0	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A flaw was found in samba 4.0.0 before samba 4.9.15 and samba 4.10.x before 4.10.10. An attacker can crash AD DC LDAP server via dirsync resulting in denial of service. Privilege escalation is not possible with this issue.
CVE-2020-1073	4.0	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A NULL pointer dereference, or possible use-after-free flaw was found in Samba AD LDAP server in versions before 4.10.17, before 4.11.11 and before 4.12.4. Although some versions of Samba shipped with Red Hat Enterprise Linux do not support Samba in AD mode, the affected code is shipped with the libldb package. This flaw allows an authenticated user to possibly trigger a use-after-free or NULL pointer dereference. The highest threat from this vulnerability is to system availability.
CVE-2020-1076	4.0	445	netbios- ssn	Samba smbd 4.6.2	2022-02-27 2023-05-06	A use-after-free flaw was found in all samba LDAP server versions before 4.10.17, before 4.11.11, before 4.12.4 used in a AC DC configuration. A Samba LDAP user could use this flaw to crash samba.

CVE-2020-14318	4.0	445 netbios- ssn	Samba smbd 4.6.2	smbd 2022-02-27 2023-05-06 A flaw was found in the way samba handled file and directory permissions. An authenticated user could use to gain access to certain file and directory information which otherwise would be unavailable to the attacker.							
CVE-2020-14383	4.0	445 netbios- ssn	Samba smbd 4.6.2		6 A flaw was found in samba's DNS server. An authenticated user could use this flaw to the RPC server to crash. This RPC server, which also serves protocols other than dnsserver, will be restarted after a short delay, but it is easy for an authenticated non administrative attacker to crash it again as soon as it returns. The Samba DNS server itself will continue to operate, but many RPC services will not.						
CVE-2020-35652	4.0	5060 sip- proxy	Asterisk PBX 16.12.0		06 An issue was discovered in res_pjsip_diversion.c in Sangoma Asterisk before 13.38.0, 14.x through 16.x before 16.15.0, 17.x before 17.9.0, and 18.x before 18.1.0. A crash can occur when a SIP message is received with a History-Info header that contains a tel-uri, or when a SIP 181 response is received that contains a tel-uri in the Diversion header.						
CVE-2021-26713 General Security Iss Severity Des		5060 sip-	Asterisk PBX		hafara 10 2	1 and Cartified Act		ngoma Asterisk before 16.16.1, 17.x before 17.9  Remediation			
Show (wit	hout e	ncryption)		e data sent plaintext e inactionable and are thu	21 ftp s <i>excluded fr</i>	vsftpd 3.0.5	2022-03-04 2023-04-19	disable FTP and migrate to secure STFP or SCP protocol			

Showing 19 hosts.