



# Hawk CVE Scanner Version 1.2

FlockBox Advanced Networking and Design

**Customer** FlockBox ??  
**Location** Ranch ??  
**Contact** Joey Kelly  
[Normal View?](#)

## Host Summary

IP	Hostname	Operating System	OS Version	CPE	NIC Vendor	First Seen	Last Seen	CVE Scores					General Security Issues			
								Critical	High	Medium	Low	Total	Critical	High	Medium	Total
192.168.2.1 ??	nathan.bibleheroes	Unix				2022-02-27	2023-05-26	73	11	84			1	1		
192.168.2.56 ??	proxmox					2023-04-27	2023-05-26	4	1	5						
192.168.2.84 ??	ciscophone.bibleheroes			cpe:/h:cisco:spa504g	Cisco Systems	2022-02-27	2023-05-26									
192.168.2.88 ??	freekde	FreeBSD		cpe:/o:freebsd:freebsd	(Oracle VirtualBox virtual NIC)	2022-02-27	2023-05-24	7	7	14						
192.168.2.112 ??	win10two	Windows		cpe:/o:microsoft:windows		2023-04-27	2023-05-24									
192.168.2.113 ??	freebsd131pve	FreeBSD		cpe:/o:freebsd:freebsd		2023-04-27	2023-05-26	1	1	2						
192.168.2.114 ??	slack15pve					2023-04-26	2023-05-26									
192.168.2.123 ??	slackchin				(Intel Corporate)	2022-02-27	2023-05-26	10	6	16						
192.168.2.150 ??					Motorola Mobility LLC a Lenovo Company	2022-03-02	2023-05-26									
192.168.2.152 ??	blackpi3wifi	FreeBSD		cpe:/o:freebsd:freebsd	(Tp-link Technologies)	2022-02-27	2023-05-26	18	6	24						
192.168.2.167 ??	blackpi3	FreeBSD		cpe:/o:freebsd:freebsd	(Raspberry Pi Foundation)	2022-02-27	2023-05-26	18	6	24						
192.168.2.171 ??						2023-04-26	2023-05-06									
192.168.2.172 ??					(Samsung Electronics)	2023-04-26	2023-05-26									
192.168.2.174 ??						2023-04-27	2023-05-24									
192.168.2.175 ??						2023-05-21	2023-05-24									
192.168.2.176 ??						2023-05-21	2023-05-24									
192.168.2.177 ??	opensuse					2023-05-21	2023-05-24	4	1	5						
192.168.2.185 ??	slack15pve2					2023-04-26	2023-05-26									
192.168.2.186 ??	devuanraid	Linux		cpe:/o:linux:linux_kernel	(Ubiquiti Networks)	2023-04-26	2023-05-26									
192.168.2.188 ??						2023-04-26	2023-05-24									
192.168.2.189 ??						2023-04-26	2023-05-24									
192.168.2.220 ??	220nathan	Unix				2022-02-27	2023-05-06	2	11	63	21	97	1	1		

Showing 22 hosts  
with 271 CVE Scores (2 Critical, 11 High, 198 Medium, 60 Low)  
and 2 General Security Issues (0 Critical, 0 High, 2 Medium) .

## Host Detail

### 192.168.2.1

**Hostname** nathan.bibleheroes  
**Operating System** Unix  
**OS Version**  
**CPE**  
**NIC Vendor**  
**First Seen** 2022-02-27  
**Last Seen** 2023-05-26  
**Critical CVSS**  
**HIGH CVSS**  
**MEDIUM CVSS** 73  
**LOW CVSS** 11  
**CVSS Total** 84

## Ports

Number	Protocol	Service	Service Version	CPE	Has Exploits?	Verified Service	Verified Version	First Seen	Last Seen
21	tcp	ftp	vsftpd 3.0.5					2022-03-02	2023-05-26
25	tcp	smtp	Postfix smtpd					2022-02-27	2023-05-26
53	tcp	domain	(unknown banner: Apache 1.3)					2022-02-27	2023-05-26
67	udp	dhcpc						2023-04-27	2023-05-26
68	udp	dhcpc						2023-04-27	2023-05-26
79	tcp	finger	BSD fingerd					2023-04-27	2023-05-26
80	tcp	http	Apache httpd 2.4.57 ((Unix) PHP/7.4.33 mod_apreq2-20101207/2.8.1 mod_perl/2.0.12 Perl/v5.34.0)					2022-02-27	2023-05-26
123	udp	ntp?						2023-04-27	2023-05-26
139	tcp	netbios-ssn	Samba smbdc 4.6.2	cpe:/a:samba:samba:4.6.2:	Yes		Samba 4.15.13	2022-02-27	2023-05-26
161	udp	snmp	net-snmp; net-snmp SNMPv3 server					2023-04-27	2023-05-26

357	tcp	ssh	OpenSSH 9.3 (protocol 2.0)						2022-02-27	2023-05-26
445	tcp	netbios-ssn	Samba smb 4.6.2	cpe:/a:samba:samba:4.6.2:	Yes	Samba 4.15.13			2022-02-27	2023-05-26
515	tcp	printer							2022-02-27	2023-05-26
1716	tcp	tcpwrapped							2022-02-27	2023-05-26
5060	udp	sip-proxy	Asterisk PBX 16.12.0	cpe:/a:digium:asterisk:16.12.0:					2023-04-27	2023-05-26
33892	tcp	ms-wbt-server	VirtualBox VM Remote Desktop Service						2023-04-27	2023-05-24

Showing 16 results.

CVE Scores

CVE	CVSS	Port	Service	Service Version	First Seen	Last Seen	Description
CVE-2017-7494 <small>Exclusion Reason: WRONGVERSION</small>	10.0	139	netbios-ssn	Samba smb 4.6.2	2022-02-27	2023-05-26	Samba since version 3.5.0 and before 4.6.4, 4.5.10 and 4.4.14 is vulnerable to remote code execution vulnerability, allowing a malicious client to upload a shared library to a writable share, and then cause the server to load and execute it.
CVE-2017-7494 <small>Exclusion Reason: WRONGVERSION</small>	10.0	445	netbios-ssn	Samba smb 4.6.2	2022-02-27	2023-05-26	Samba since version 3.5.0 and before 4.6.4, 4.5.10 and 4.4.14 is vulnerable to remote code execution vulnerability, allowing a malicious client to upload a shared library to a writable share, and then cause the server to load and execute it.
CVE-2020-17049 <small>Exclusion Reason: NOTIMPLEMENTED</small>	9.0	139	netbios-ssn	Samba smb 4.6.2	2023-04-27	2023-05-26	Kerberos Security Feature Bypass Vulnerability
CVE-2020-25719 <small>Exclusion Reason: NOTIMPLEMENTED</small>	9.0	139	netbios-ssn	Samba smb 4.6.2	2022-03-02	2023-05-26	A flaw was found in the way Samba, as an Active Directory Domain Controller, implemented Kerberos name-based authentication. The Samba AD DC, could become confused about the user a ticket represents if it did not strictly require a Kerberos PAC and always use the SIDs found within. The result could include total domain compromise.
CVE-2020-17049 <small>Exclusion Reason: NOTIMPLEMENTED</small>	9.0	445	netbios-ssn	Samba smb 4.6.2	2023-04-27	2023-05-26	Kerberos Security Feature Bypass Vulnerability
CVE-2020-25719 <small>Exclusion Reason: NOTIMPLEMENTED</small>	9.0	445	netbios-ssn	Samba smb 4.6.2	2022-03-02	2023-05-26	A flaw was found in the way Samba, as an Active Directory Domain Controller, implemented Kerberos name-based authentication. The Samba AD DC, could become confused about the user a ticket represents if it did not strictly require a Kerberos PAC and always use the SIDs found within. The result could include total domain compromise.
CVE-2020-25717 <small>Exclusion Reason: NOTIMPLEMENTED</small>	8.5	139	netbios-ssn	Samba smb 4.6.2	2022-02-27	2023-05-26	A flaw was found in the way Samba maps domain users to local users. An authenticated attacker could use this flaw to cause possible privilege escalation.
CVE-2020-25717 <small>Exclusion Reason: NOTIMPLEMENTED</small>	8.5	445	netbios-ssn	Samba smb 4.6.2	2022-02-27	2023-05-26	A flaw was found in the way Samba maps domain users to local users. An authenticated attacker could use this flaw to cause possible privilege escalation.
CVE-2020-10745 <small>Exclusion Reason: WRONGVERSION</small>	7.8	139	netbios-ssn	Samba smb 4.6.2	2022-02-27	2023-05-26	A flaw was found in all Samba versions before 4.10.17, before 4.11.11 and before 4.12.4 in the way it processed NetBios over TCP/IP. This flaw allows a remote attacker could to cause the Samba server to consume excessive CPU use, resulting in a denial of service. This highest threat from this vulnerability is to system availability.
CVE-2020-10745 <small>Exclusion Reason: WRONGVERSION</small>	7.8	445	netbios-ssn	Samba smb 4.6.2	2022-02-27	2023-05-26	A flaw was found in all Samba versions before 4.10.17, before 4.11.11 and before 4.12.4 in the way it processed NetBios over TCP/IP. This flaw allows a remote attacker could to cause the Samba server to consume excessive CPU use, resulting in a denial of service. This highest threat from this vulnerability is to system availability.
CVE-2017-14746 <small>Exclusion Reason: WRONGVERSION</small>	7.5	139	netbios-ssn	Samba smb 4.6.2	2022-02-27	2023-05-26	Use-after-free vulnerability in Samba 4.x before 4.7.3 allows remote attackers to execute arbitrary code via a crafted SMB1 request.
CVE-2017-14746 <small>Exclusion Reason: WRONGVERSION</small>	7.5	445	netbios-ssn	Samba smb 4.6.2	2022-02-27	2023-05-26	Use-after-free vulnerability in Samba 4.x before 4.7.3 allows remote attackers to execute arbitrary code via a crafted SMB1 request.
CVE-2022-26651 <small>Exclusion Reason: NOTENABLED</small>	7.5	5060	sip-proxy	Asterisk PBX 16.12.0	2023-04-27	2023-05-26	An issue was discovered in Asterisk through 19.x and Certified Asterisk through 16.8-cert13. The func_odbc module provides possibly inadequate escaping functionality for backslash characters in SQL queries, resulting in user-provided data creating a broken SQL query or possibly a SQL injection. This is fixed in 16.25.2, 18.11.2, and 19.3.2, and 16.8-cert14.
CVE-2017-11103	6.8	139	netbios-ssn	Samba smb 4.6.2	2022-02-27	2023-05-26	Heimdal before 7.4 allows remote attackers to impersonate services with Orpheus' Lyre attacks because it obtains service-principal names in a way that violates the Kerberos 5 protocol specification. In _krb5_extract_ticket() the KDC-REP service name must be obtained from the encrypted version stored in 'enc_part' instead of the unencrypted version stored in 'ticket'. Use of the unencrypted version provides an opportunity for successful server impersonation and other attacks. NOTE: this CVE is only for Heimdal and other products that embed Heimdal code; it does not apply to other instances in which this part of the Kerberos 5 protocol specification is violated.
CVE-2017-11103	6.8	445	netbios-ssn	Samba smb 4.6.2	2022-02-27	2023-05-26	Heimdal before 7.4 allows remote attackers to impersonate services with Orpheus' Lyre attacks because it obtains service-principal names in a way that violates the Kerberos 5 protocol specification. In _krb5_extract_ticket() the KDC-REP service name must be obtained from the encrypted version stored in 'enc_part' instead of the unencrypted version stored in 'ticket'. Use of the unencrypted version provides an opportunity for successful server impersonation and other attacks. NOTE: this CVE is only for Heimdal and other products that embed Heimdal code; it does not apply to other instances in which this part of the Kerberos 5 protocol specification is violated.
CVE-2018-1057	6.5	139	netbios-ssn	Samba smb 4.6.2	2023-04-27	2023-05-26	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	139	netbios-ssn	Samba smb 4.6.2	2022-02-27	2023-05-26	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 smb 4.6.2	2022-03-02	2023-05-26	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 smb 4.6.2	2022-02-27	2023-05-26	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 smb 4.6.2	2022-03-13	2023-05-26	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-2022-0336	6.5	139	netbios-ssn	Samba smb 4.6.2	2023-04-27	2023-05-26	The Samba AD DC includes checks when adding service principals names (SPNs) to an account to ensure that SPNs do not alias with those already in the database. Some of these checks are able to be bypassed if an account modification re-adds an SPN that was previously present on that account, such as one added when a computer is joined to a domain. An attacker who has the ability to write to an account can exploit this to perform a denial-of-service attack by adding an SPN that matches an existing service. Additionally, an attacker who can intercept traffic can impersonate existing services, resulting in a loss of confidentiality and integrity.
CVE-2022-32744	6.5	139	netbios-ssn	Samba smb 4.6.2	2023-04-27	2023-05-26	A flaw was found in Samba. The KDC accepts kpasswd requests encrypted with any key known to it. By encrypting forged kpasswd requests with its own key, a user can change other users' passwords, enabling full domain takeover.
CVE-2018-1057	6.5	445	netbios-ssn	Samba smb 4.6.2	2023-04-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-03-02	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-03-13	2023-05-26	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-2022-0336	6.5	445	netbios-ssn	Samba smbdc 4.6.2	2023-04-27	2023-05-26	The Samba AD DC includes checks when adding service principals names (SPNs) to an account to ensure that SPNs do not alias with those already in the database. Some of these checks are able to be bypassed if an account modification re-adds an SPN that was previously present on that account, such as one added when a computer is joined to a domain. An attacker who has the ability to write to an account can exploit this to perform a denial-of-service attack by adding an SPN that matches an existing service. Additionally, an attacker who can intercept traffic can impersonate existing services, resulting in a loss of confidentiality and integrity.
CVE-2022-32744	6.5	445	netbios-ssn	Samba smbdc 4.6.2	2023-04-27	2023-05-26	A flaw was found in Samba. The KDC accepts kpasswd requests encrypted with any key known to it. By encrypting forged kpasswd requests with its own key, a user can change other users' passwords, enabling full domain takeover.
CVE-2019-14870	6.4	139	netbios-ssn	Samba smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2023-04-27	2023-05-26	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 smbdc 4.6.2	2023-04-27	2023-05-26	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-2022-32746	5.5	139	netbios-ssn	Samba smbdc 4.6.2	2023-04-27	2023-05-26	A flaw was found in the Samba AD LDAP server. The AD DC database audit logging module can access LDAP message values freed by a preceding database module, resulting in a use-after-free issue. This issue is only possible when modifying certain privileged attributes, such as userAccountControl.
CVE-2019-14902	5.5	445	netbios-ssn	Samba smbdc 4.6.2	2023-04-27	2023-05-26	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 smbdc 4.6.2	2023-04-27	2023-05-26	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-2022-32746	5.5	445	netbios-ssn	Samba smbdc 4.6.2	2023-04-27	2023-05-26	A flaw was found in the Samba AD LDAP server. The AD DC database audit logging module can access LDAP message values freed by a preceding database module, resulting in a use-after-free issue. This issue is only possible when modifying certain privileged attributes, such as userAccountControl.
CVE-2017-15275	5.0	139	netbios-ssn	Samba smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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	2023-05-26	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	2023-05-26	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	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	A flaw was found in samba. The Samba smbdc 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 smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	A flaw was found in samba. The Samba smbdc 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 smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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	sip-proxy	Asterisk PBX 16.12.0	2023-04-27	2023-05-26	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	sip-proxy	Asterisk PBX 16.12.0	2023-04-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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	139	netbios-ssn	Samba smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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-2022-3437	4.0	139	netbios-ssn	Samba smbdc 4.6.2	2023-04-27	2023-05-26	A heap-based buffer overflow vulnerability was found in Samba within the GSSAPI unwrap_des() and unwrap_des3() routines of Heimdal. The DES and Triple-DES decryption routines in the Heimdal GSSAPI library allow a length-limited write buffer overflow on malloc() allocated memory when presented with a maliciously small packet. This flaw allows a remote user to send specially crafted malicious data to the application, possibly resulting in a denial of service (DoS) attack.
CVE-2023-0614	4.0	139	netbios-ssn	Samba smbdc 4.6.2	2023-04-27	2023-05-26	The fix in 4.6.16, 4.7.9, 4.8.4 and 4.9.7 for CVE-2018-10919 Confidential attribute disclosure via LDAP filters was insufficient and an attacker may be able to obtain confidential BitLocker recovery keys from a Samba AD DC.
CVE-2018-10919	4.0	445	netbios-ssn	Samba smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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 dirsyntax resulting in denial of service. Privilege escalation is not possible with this issue.
CVE-2020-10730	4.0	445	netbios-ssn	Samba smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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 smbdc 4.6.2	2022-02-27	2023-05-26	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-2022-3437	4.0	445	netbios-ssn	Samba smbdc 4.6.2	2023-04-27	2023-05-26	A heap-based buffer overflow vulnerability was found in Samba within the GSSAPI unwrap_des() and unwrap_des3() routines of Heimdal. The DES and Triple-DES decryption routines in the Heimdal GSSAPI library allow a length-limited write buffer overflow on malloc() allocated memory when presented with a maliciously small packet. This flaw allows a remote user to send specially crafted malicious data to the application, possibly resulting in a denial of service (DoS) attack.
CVE-2023-0614	4.0	445	netbios-ssn	Samba smbdc 4.6.2	2023-04-27	2023-05-26	The fix in 4.6.16, 4.7.9, 4.8.4 and 4.9.7 for CVE-2018-10919 Confidential attribute disclosure via LDAP filters was insufficient and an attacker may be able to obtain confidential BitLocker recovery keys from a Samba AD DC.
CVE-2020-35652	4.0	5060	sip-proxy	Asterisk PBX 16.12.0	2023-04-27	2023-05-26	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	4.0	5060	sin	Asterisk PBX 16.12.0	2023-04-27	2023-05-26	A use-after-free vulnerability was found in res_rtp_asterisk.c in Sangoma Asterisk before 16.16.1, 17.x before 17.9.0, and 18.x before 18.1.0. An attacker could use this flaw to crash the application.
<b>General Security Issues</b>							
<b>Severity</b>	<b>Description</b>	<b>Port</b>	<b>Service</b>	<b>Service Version</b>	<b>First Seen</b>	<b>Last Seen</b>	<b>Remediation</b>
MEDIUM	FTP sends passwords and/or other sensitive data sent plaintext (without encryption)	21	ftp	vsftpd 3.0.5	2022-03-02	2023-05-21	disable FTP and migrate to secure SFTP or SCP protocol
<b>Note: Low-ranked results are informational-only or otherwise actionable and are thus excluded from this listing.</b>							
Showing 1 results.							

192.168.2.56

**Hostname** proxmox  
**Operating System**  
**OS Version**  
**CPE**  
**NIC Vendor**  
**First Seen** 2023-04-27  
**Last Seen** 2023-05-26  
**Critical CVSS**  
**HIGH CVSS**  
**MEDIUM CVSS** 4  
**LOW CVSS** 1  
**CVSS Total** 5

Ports

Number	Protocol	Service	Service Version	CPE	Has Exploits?	Verified Service	Verified Version	First Seen	Last Seen
22	tcp	ssh	OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)	cpe:/a:openssh:openssh:8.4p1:				2023-04-27	2023-05-26
22	tcp	ssh	OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)	cpe:/a:openssh:openssh:8.4p1:				2023-05-21	2023-05-26
111	tcp	rpcbind	2-4 (RPC #100000)					2023-04-27	2023-05-26
111	tcp	rpcbind	2-4 (RPC #100000)					2023-05-21	2023-05-26
111	udp	rpcbind	2-4 (RPC #100000)					2023-05-21	2023-05-26
3128	tcp	http	Proxmox Virtual Environment REST API 3.0					2023-04-27	2023-05-26
3128	tcp	http	Proxmox Virtual Environment REST API 3.0					2023-05-21	2023-05-26
8006	tcp	wpl-analytics?						2023-04-27	2023-05-26
8006	tcp	wpl-analytics?						2023-05-21	2023-05-26

Showing 9 results.

CVE Scores

CVE	CVSS	Port	Service	Service Version	First Seen	Last Seen	Description
CVE-2021-28041	4.6	22	ssh	OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)	2023-04-27	2023-05-06	ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.
CVE-2021-41617	4.4	22	ssh	OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)	2023-04-27	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-2016-20012	4.3	22	ssh	OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)	2023-04-27	2023-05-06	** DISPUTED ** OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.
CVE-2020-14145	4.3	22	ssh	OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)	2023-04-27	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.

Showing 4 results.

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