YourIT!
Your Logo Goes Here

VulScan

Internal Vulnerability Scan Issues by Device

CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Prepared for: Client Company

Prepared by: YourIT Company

05/04/2022

Table of Contents

01 Summary

02 Details

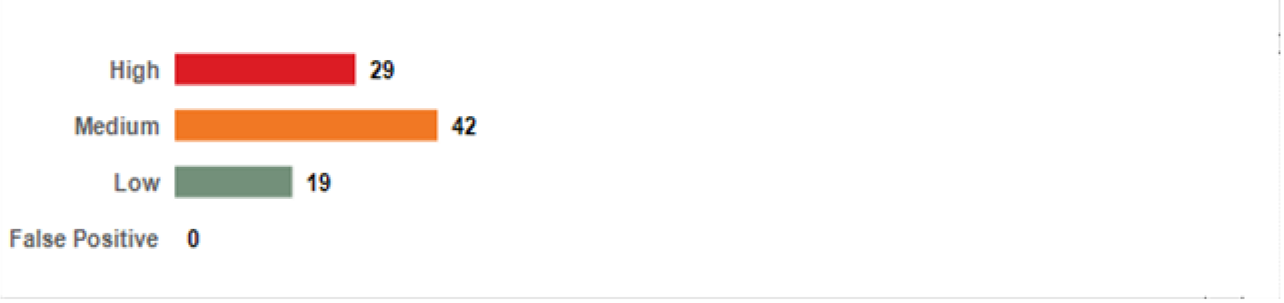
2.1 176.16.1.57 (00:17:4G:01:07:B6)
2.2 176.16.1.58 (00:17:4G:01:07:CC)
2.3 176.16.1.59 (00:17:4G:01:07:C3)
2.4 176.16.1.64 (00:17:4G:01:07:C5)
2.5 176.16.1.65 (00:17:4G:01:07:C6)
2.6 176.16.1.67 (00:17:4G:01:07:C8)
2.7 176.16.1.70 (B0:26:28:B6:DC:4F)
2.8 deskpc-0o3l5bq.myco.com (176.16.1.73 / 00:17:4G:01:08:38)
2.9 sql03.myco.com (176.16.1.107 / 00:17:4G:01:07:32)
2.10 176.16.1.147 (B0:26:28:B6:C6:4C)
2.11 176.16.1.148 (B0:26:28:B6:DC:4E)
2.12 176.16.1.156 (00:17:4G:01:07:7B)
2.13 deskpc-f6ckerq.myco.com (176.16.1.171 / 00:17:4G:01:08:02)
2.14 176.16.1.178 (00:17:4G:01:07:94)
2.15 win-tatvq3rem1k.myco.com (176.16.1.211 / 00:17:4G:01:07:B3)
2.16 deskpc-07rd86g.myco.com (176.16.1.213 / 00:17:4G:01:08:31)
2.17 176.16.1.219 (00:17:4G:01:08:32)
2.18 176.16.1.54 (00:17:4G:01:07:BE)
2.19 dctrlr01.myco.com (176.16.1.12 / 00:17:4G:01:07:19)
2.20 dctrlr02.myco.com (176.16.1.13 / 00:17:4G:01:07:1A)
2.21 appsvr01.myco.com (176.16.1.14 / 00:17:4G:01:07:18)
2.22 exchsvr01.myco.com (176.16.1.15 / 00:17:4G:01:07:24)
2.23 fsvr01.myco.com (176.16.1.16 / 00:17:4G:01:07:1B)
2.24 sql01.myco.com (176.16.1.17 / 00:17:4G:01:07:1D)
2.25 176.16.1.71 (F4:8E:38:20:FD:F4)

2.26 176.16.1.108 (00:17:4G:01:08:0C)
2.27 176.16.1.185 (00:17:4G:01:08:0E)
2.28 176.16.1.186 (00:17:4G:01:08:11)
2.29 176.16.1.188 (00:17:4G:01:08:1D)
2.30 176.16.1.189 (00:17:4G:01:08:14)
2.31 176.16.1.208 (00:17:4G:01:07:A0)

1 - Summary

This report gives details on hosts that were tested and issues that were found.

Issues by Severity



Results Filter

Scan Date Range:	04/03/2022 - 05/03/2022
CVSS Filter:	Low (1.0+)
Scan Type:	Internal

Components Scanned

IP Address	Hostname	MAC Address
176.16.1.12	dctrlr01.myco.com	00:17:4G:01:07:19
176.16.1.13	dctrlr02.myco.com	00:17:4G:01:07:1A
176.16.1.14	appsvr01.myco.com	00:17:4G:01:07:18
176.16.1.15	exchsvr01.myco.com	00:17:4G:01:07:24
176.16.1.16	fsvr01.myco.com	00:17:4G:01:07:1B
176.16.1.17	sql01.myco.com	00:17:4G:01:07:1D
176.16.1.54		00:17:4G:01:07:BE
176.16.1.57		00:17:4G:01:07:B6
176.16.1.58		00:17:4G:01:07:CC
176.16.1.59		00:17:4G:01:07:C3

IP Address	Hostname	MAC Address
176.16.1.64		00:17:4G:01:07:C5
176.16.1.65		00:17:4G:01:07:C6
176.16.1.67		00:17:4G:01:07:C8
176.16.1.70		B0:26:28:B6:DC:4F
176.16.1.71		F4:8E:38:20:FD:F4
176.16.1.73	deskpc-0o3l5bq.myco.com	00:17:4G:01:08:38
176.16.1.107	sql03.myco.com	00:17:4G:01:07:32
176.16.1.108		00:17:4G:01:08:0C
176.16.1.147		B0:26:28:B6:C6:4C
176.16.1.148		B0:26:28:B6:DC:4E
176.16.1.156		00:17:4G:01:07:7B
176.16.1.171	deskpc-f6ckerq.myco.com	00:17:4G:01:08:02
176.16.1.178		00:17:4G:01:07:94
176.16.1.185		00:17:4G:01:08:0E
176.16.1.186		00:17:4G:01:08:11
176.16.1.188		00:17:4G:01:08:1D
176.16.1.189		00:17:4G:01:08:14
176.16.1.208		00:17:4G:01:07:A0
176.16.1.211	winpc-tatvq3rem1k.myco.com	00:17:4G:01:07:B3
176.16.1.213	deskpc-07rd86g.myco.com	00:17:4G:01:08:31
176.16.1.219		00:17:4G:01:08:32

2 - Scan Details

2.1 - 176.16.1.57 (00:17:4G:01:07:B6)

Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	HIGHEST CVSS
176.16.1.57 (00:17:4G:01:07:B6)	2	**2**	**2**	1	7.5

Listening Ports

PORT
22/tcp (ssh), 0/NA

Security Issues

H	HIGH (CVSS: 7.5) NVT: DIFFIE-HELLMAN EPHEMERAL KEY EXCHANGE DOS VULNERABILITY (SSH, D(HE)ATER) (OID: 1.3.6.1.4.1.25623.1.0.117839)	22/TCP (SSH)

Summary
The remote SSH server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange (KEX) algorithms and thus could be prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
The remote SSH server supports the following DHE KEX algorithm(s):diffie-hellman-group14-sha1diffie-hellman-group14-sha256diffie-hellman-group16-sha512diffie-hellman-group18-sha512diffie-hellman-group-exchange-sha256

Solution
'- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered. - Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For OpenSSH this limit can be configured via the 'MaxStartups' option, for other products please refer to the manual of the product in question on configuration possibilities.

Vulnerability Insight
The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE.

Vulnerability Detection Method
Checks the supported KEX algorithms of the remote SSH server.Details:Diffie-Hellman Ephemeral Key Exchange DoS

Vulnerability (SSH, D(HE)ater)(OID: 1.3.6.1.4.1.25623.1.0.117839)Version used: 2021-12-17T14:03:21Z

References
https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Security_Issues_in_the_Diffie-Hellman_Key_Agreement_Protocol,https://github.com/Balasys/dheater

H

HIGH (CVSS: 7)

NVT: OPENSSH 6.2 <= 8.7 PRIVILEGE ESCALATION VULNERABILITY (OID: 1.3.6.1.4.1.25623.1.0.117696)

22/TCP
(SSH)

Summary
OpenSSH is prone to a privilege scalation vulnerability in certain configurations.

Vulnerability Detection Result
Installed version: 8.1Fixed version: 8.8Installationpath / port: 22/tcp

Solution
Update to version 8.8 or later.

Vulnerability Insight
sshd failed to correctly initialise supplemental groups when executing an AuthorizedKeysCommand or AuthorizedPrincipalsCommand, where a AuthorizedKeysCommandUser or AuthorizedPrincipalsCommandUser directive has been set to run the command as a different user. Instead these commands would inherit the groups that sshd was started with. Depending on system configuration, inherited groups may allow AuthorizedKeysCommand/AuthorizedPrincipalsCommand helper programs to gain unintended privilege. Neither AuthorizedKeysCommand nor AuthorizedPrincipalsCommand are enabled by default in sshd_config.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH 6.2 <= 8.7 Privilege Escalation Vulnerability(OID: 1.3.6.1.4.1.25623.1.0.117696)Version used: 2021-10-11T08:01:31Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:8.1Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://www.openssh.com/txt/release-8.8

M

MEDIUM (CVSS: 5.9)

NVT: OPENBSD OPENSSH INFORMATION DISCLOSURE VULNERABILITY (CVE-2020-14145) (OID: 1.3.6.1.4.1.25623.1.0.117785)

22/TCP
(SSH)

Summary
OpenBSD OpenSSH is prone to an information disclosure vulnerability.

Vulnerability Detection Result
Installed version: 8.1Fixed version: 8.5Installationpath / port: 22/tcp

Solution
Update to version 8.5 or later.

Vulnerability Insight
The client side in OpenSSH 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).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenBSD OpenSSH Information Disclosure Vulnerability (CVE-2020-14145)(OID: 1.3.6.1.4.1.25623.1.0.117785)Version used: 2021-11-22T14:03:31Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:8.1Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
http://www.openwall.com/lists/oss-security/2020/12/02/1

M

MEDIUM (CVSS: 5.3)

NVT: OPENSSH INFORMATION DISCLOSURE VULNERABILITY (CVE-2016-20012) (OID: 1.3.6.1.4.1.25623.1.0.117777)

22/TCP (SSH)

Summary
OpenBSD OpenSSH is prone to an information disclosure vulnerability.

Vulnerability Detection Result
Installed version: 8.1Fixed version: NoneInstallationpath / port: 22/tcp

Solution
No known solution is available as of 16th November, 2021. Information regarding this issue will be updated once solution details are available. Note: This issue is not treated as a security issue by the vendor so no update might be provided in the future.

Vulnerability Insight
OpenSSH 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.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH Information Disclosure Vulnerability (CVE-2016-20012)(OID: 1.3.6.1.4.1.25623.1.0.117777)Version used: 2021-11-16T14:03:35Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:8.1Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://github.com/openssh/openssh-portable/pull/270,https://rushter.com/blog/public-ssh-keys/,https://utcc.utoronto.ca/~cks/space/blog/tech/SSHKeysAreInfoLeak

L

LOW (CVSS: 2.6)

NVT: TCP TIMESTAMPS (OID: 1.3.6.1.4.1.25623.1.0.80091)

0/NA

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
It was detected that the host implements RFC1323/RFC7323.The following timestamps were retrieved with a delay of 1 seconds in-between:Packet 1: 1458897013Packet 2: 1458898145

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the

settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.Details:TCP timestamps(OID: 1.3.6.1.4.1.25623.1.0.80091)Version used: 2020-08-24T08:40:10Z

References
http://www.ietf.org/rfc/rfc1323.txt,http://www.ietf.org/rfc/rfc7323.txt,https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152

2.2 - 176.16.1.58 (00:17:4G:01:07:CC)

Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	HIGHEST CVSS
176.16.1.58 (00:17:4G:01:07:CC)	4	5	2	1	7.5

Listening Ports

PORT
81/tcp, 80/tcp (http), 22/tcp (ssh), 0/NA

Security Issues

H

HIGH (CVSS: 7.5)

NVT: NGINX <= 1.21.1 INFORMATION DISCLOSURE VULNERABILITY (OID: 1.3.6.1.4.1.25623.1.0.117523)

81/TCP,80/TCP (HTTP)

Summary
nginx is prone to an information disclosure vulnerability.

Vulnerability Detection Result
Installed version: 1.18.0Fixed version: NoneInstallationpath / port: 81/tcp

Solution
No known solution is available as of 12th August, 2021. Information regarding this issue will be updated once solution details are available.

Vulnerability Insight
The default configuration of nginx uses world-readable permissions for the access.log and error.log files, which allows local

users to obtain sensitive information by reading the files.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:nginx <= 1.21.1 Information Disclosure Vulnerability(OID: 1.3.6.1.4.1.25623.1.0.117523)Version used: 2021-08-12T09:00:13Z

Product Detection Result
Product: cpe:/a:nginx:nginx:1.18.0Method: nginx Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.113787)

References
https://trac.nginx.org/nginx/ticket/376

H HIGH (CVSS: 7.5)

NVT: DIFFIE-HELLMAN EPHEMERAL KEY EXCHANGE DOS VULNERABILITY (SSH, D(HE)ATER) (OID: 1.3.6.1.4.1.25623.1.0.117839)

22/TCP (SSH)

Summary
The remote SSH server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange (KEX) algorithms and thus could be prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
The remote SSH server supports the following DHE KEX algorithm(s):diffie-hellman-group14-sha256diffie-hellman-group16-sha512diffie-hellman-group18-sha512diffie-hellman-group-exchange-sha256

Solution
'- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered. - Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For OpenSSH this limit can be configured via the 'MaxStartups' option, for other products please refer to the manual of the product in question on configuration possibilities.

Vulnerability Insight
The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE.

Vulnerability Detection Method
Checks the supported KEX algorithms of the remote SSH server.Details:Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSH, D(HE)ater)(OID: 1.3.6.1.4.1.25623.1.0.117839)Version used: 2021-12-17T14:03:21Z

References
https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Security_Issues_in_the_Diffie-Hellman_Key_Agreement_Protocol,https://github.com/Balasys/dheater

H HIGH (CVSS: 7.1)

NVT: OPENSSH 8.2 < 8.5 MEMORY CORRUPTION VULNERABILITY (OID: 1.3.6.1.4.1.25623.1.0.145538)

22/TCP (SSH)

Summary
OpenSSH is prone to a memory corruption vulnerability in the ssh-agent.

Vulnerability Detection Result

Installed version: 8.2p1Fixed version: 8.5Installationpath / port: 22/tcp

Solution
Update to version 8.5 or later.

Vulnerability Insight
ssh-agent in OpenSSH 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.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH 8.2 < 8.5 Memory Corruption Vulnerability(OID: 1.3.6.1.4.1.25623.1.0.145538)Version used: 2021-08-17T12:00:57Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:8.2p1Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://www.openssh.com/txt/release-8.5

H

HIGH (CVSS: 7)

NVT: OPENSSH 6.2 <= 8.7 PRIVILEGE ESCALATION VULNERABILITY (OID: 1.3.6.1.4.1.25623.1.0.117696)

22/TCP (SSH)

Summary
OpenSSH is prone to a privilege scalation vulnerability in certain configurations.

Vulnerability Detection Result
Installed version: 8.2p1Fixed version: 8.8Installationpath / port: 22/tcp

Solution
Update to version 8.8 or later.

Vulnerability Insight
sshd failed to correctly initialise supplemental groups when executing an AuthorizedKeysCommand or AuthorizedPrincipalsCommand, where a AuthorizedKeysCommandUser or AuthorizedPrincipalsCommandUser directive has been set to run the command as a different user. Instead these commands would inherit the groups that sshd was started with. Depending on system configuration, inherited groups may allow AuthorizedKeysCommand/AuthorizedPrincipalsCommand helper programs to gain unintended privilege. Neither AuthorizedKeysCommand nor AuthorizedPrincipalsCommand are enabled by default in sshd_config.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH 6.2 <= 8.7 Privilege Escalation Vulnerability(OID: 1.3.6.1.4.1.25623.1.0.117696)Version used: 2021-10-11T08:01:31Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:8.2p1Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://www.openssh.com/txt/release-8.8

M

MEDIUM (CVSS: 5.9)

NVT: OPENBSD OPENSSH INFORMATION DISCLOSURE VULNERABILITY (CVE-2020-14145) (OID: 1.3.6.1.4.1.25623.1.0.117785)

22/TCP (SSH)

Summary
OpenBSD OpenSSH is prone to an information disclosure vulnerability.

Vulnerability Detection Result
Installed version: 8.2p1Fixed version: 8.5Installationpath / port: 22/tcp

Solution
Update to version 8.5 or later.

Vulnerability Insight
The client side in OpenSSH 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).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenBSD OpenSSH Information Disclosure Vulnerability (CVE-2020-14145)(OID: 1.3.6.1.4.1.25623.1.0.117785)Version used: 2021-11-22T14:03:31Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:8.2p1Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
http://www.openwall.com/lists/oss-security/2020/12/02/1

M

MEDIUM (CVSS: 5.3)

NVT: OPENSSH INFORMATION DISCLOSURE VULNERABILITY (CVE-2016-20012) (OID: 1.3.6.1.4.1.25623.1.0.117777)

22/TCP (SSH)

Summary
OpenBSD OpenSSH is prone to an information disclosure vulnerability.

Vulnerability Detection Result
Installed version: 8.2p1Fixed version: NoneInstallationpath / port: 22/tcp

Solution
No known solution is available as of 16th November, 2021. Information regarding this issue will be updated once solution details are available. Note: This issue is not treated as a security issue by the vendor so no update might be provided in the future.

Vulnerability Insight
OpenSSH 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.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH Information Disclosure Vulnerability (CVE-2016-20012)(OID: 1.3.6.1.4.1.25623.1.0.117777)Version used: 2021-11-16T14:03:35Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:8.2p1Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://github.com/openssh/openssh-portable/pull/270,https://rushter.com/blog/public-ssh-keys/,https://utcc.utoronto.ca/~cks/space/blog/tech/SSHKeysAreInfoLeak

L

LOW (CVSS: 2.6)

NVT: TCP TIMESTAMPS (OID: 1.3.6.1.4.1.25623.1.0.80091)

0/NA

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
It was detected that the host implements RFC1323/RFC7323.The following timestamps were retrieved with a delay of 1 seconds in-between:Packet 1: 1682412026Packet 2: 1682413151

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.Details:TCP timestamps(OID: 1.3.6.1.4.1.25623.1.0.80091)Version used: 2020-08-24T08:40:10Z

References
http://www.ietf.org/rfc/rfc1323.txt,http://www.ietf.org/rfc/rfc7323.txt,https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152

2.3 - 176.16.1.59 (00:17:4G:01:07:C3)

Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	HIGHEST CVSS
176.16.1.59 (00:17:4G:01:07:C3)	2	2	8	1	7.5

Listening Ports

PORT
22/tcp (ssh), 0/NA

Security Issues

H	HIGH (CVSS: 7.5) NVT: DIFFIE-HELLMAN EPHEMERAL KEY EXCHANGE DOS VULNERABILITY (SSH, D(HE)ATER) (OID: 1.3.6.1.4.1.25623.1.0.117839)	22/TCP (SSH)

Summary
The remote SSH server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange (KEX) algorithms and thus could be prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
The remote SSH server supports the following DHE KEX algorithm(s):diffie-hellman-group1-sha1diffie-hellman-group14-sha1diffie-hellman-group14-sha256diffie-hellman-group16-sha512diffie-hellman-group18-sha512diffie-hellman-group-exchange-sha1diffie-hellman-group-exchange-sha256

Solution
'- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered. - Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For OpenSSH this limit can be configured via the 'MaxStartups' option, for other products please refer to the manual of the product in question on configuration possibilities.

Vulnerability Insight
The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE.

Vulnerability Detection Method
Checks the supported KEX algorithms of the remote SSH server.Details:Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSH, D(HE)ater)(OID: 1.3.6.1.4.1.25623.1.0.117839)Version used: 2021-12-17T14:03:21Z

References
https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Security_Issues_in_the_Diffie-Hellman_Key_Agreement_Protocol,https://github.com/Balasys/dheater

H

HIGH (CVSS: 7)

NVT: OPENSSH 6.2 <= 8.7 PRIVILEGE ESCALATION VULNERABILITY (OID: 1.3.6.1.4.1.25623.1.0.117696)

22/TCP (SSH)

Summary
OpenSSH is prone to a privilege scalation vulnerability in certain configurations.

Vulnerability Detection Result
Installed version: 7.4Fixed version: 8.8Installationpath / port: 22/tcp

Solution
Update to version 8.8 or later.

Vulnerability Insight
sshd failed to correctly initialise supplemental groups when executing an AuthorizedKeysCommand or AuthorizedPrincipalsCommand, where a AuthorizedKeysCommandUser or AuthorizedPrincipalsCommandUser directive has been set to run the command as a different user. Instead these commands would inherit the groups that sshd was started with. Depending on system configuration, inherited groups may allow AuthorizedKeysCommand/AuthorizedPrincipalsCommand helper programs to gain unintended privilege. Neither AuthorizedKeysCommand nor AuthorizedPrincipalsCommand are enabled by default in sshd_config.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH 6.2 <= 8.7 Privilege Escalation Vulnerability(OID: 1.3.6.1.4.1.25623.1.0.117696)Version used: 2021-10-11T08:01:31Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.4Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://www.openssh.com/txt/release-8.8

M

MEDIUM (CVSS: 5.9)

NVT: OPENBSD OPENSSH <= 7.9 MULTIPLE VULNERABILITIES (OID: 1.3.6.1.4.1.25623.1.0.117786)

22/TCP (SSH)

Summary
OpenBSD OpenSSH is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 7.4Fixed version: 8.0Installationpath / port: 22/tcp

Solution
Update to version 8.0 or later.

Vulnerability Insight
The following flaws exist: - CVE-2018-20685: bypass of intended access restrictions in the scp client - CVE-2019-6109, CVE-2019-6110: manipulation of the output in the scp client by a malicious server - CVE-2019-6111: overwrite of arbitrary files in the scp client by a malicious server

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenBSD OpenSSH <= 7.9 Multiple Vulnerabilities(OID: 1.3.6.1.4.1.25623.1.0.117786)Version used: 2021-11-22T14:03:31Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.4Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://sintonen.fi/advisories/scp-client-multiple-vulnerabilities.txt,http://www.openwall.com/lists/oss-security/2019/04/18/1

M

MEDIUM (CVSS: 5.9)

NVT: OPENBSD OPENSSH INFORMATION DISCLOSURE VULNERABILITY (CVE-2020-14145) (OID: 1.3.6.1.4.1.25623.1.0.117785)

22/TCP (SSH)

Summary
OpenBSD OpenSSH is prone to an information disclosure vulnerability.

Vulnerability Detection Result
Installed version: 7.4Fixed version: 8.5Installationpath / port: 22/tcp

Solution
Update to version 8.5 or later.

Vulnerability Insight
The client side in OpenSSH 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).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenBSD OpenSSH Information Disclosure Vulnerability (CVE-2020-14145)(OID: 1.3.6.1.4.1.25623.1.0.117785)Version used: 2021-11-22T14:03:31Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.4Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
http://www.openwall.com/lists/oss-security/2020/12/02/1

MEDIUM (CVSS: 5.3)

NVT: OPENSSH SFTP-SERVER SECURITY BYPASS VULNERABILITY (LINUX) (OID: 1.3.6.1.4.1.25623.1.0.812051)

22/TCP (SSH)

Summary
openssh is prone to a security bypass vulnerability.

Vulnerability Detection Result
Installed version: 7.4Fixed version: 7.6Installationpath / port: 22/tcp

Impact
Successfully exploiting this issue allows local users to bypass certain security restrictions and perform unauthorized actions. This may lead to further attacks.

Solution
Upgrade to OpenSSH version 7.6 or later.

Vulnerability Insight
The flaw exists in the 'process_open' function in sftp-server.c script which does not properly prevent write operations in readonly mode.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH 'sftp-server' Security Bypass Vulnerability (Linux)(OID: 1.3.6.1.4.1.25623.1.0.812051)Version used: 2022-04-13T11:57:07Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.4Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://www.openssh.com/txt/release-7.6,https://github.com/openbsd/src/commit/a6981567e8e

MEDIUM (CVSS: 5.3)

NVT: OPENSSH INFORMATION DISCLOSURE VULNERABILITY (CVE-2016-20012) (OID: 1.3.6.1.4.1.25623.1.0.117777)

22/TCP (SSH)

Summary
OpenBSD OpenSSH is prone to an information disclosure vulnerability.

Vulnerability Detection Result
Installed version: 7.4Fixed version: NoneInstallationpath / port: 22/tcp

Solution
No known solution is available as of 16th November, 2021. Information regarding this issue will be updated once solution details are available. Note: This issue is not treated as a security issue by the vendor so no update might be provided in the future.

Vulnerability Insight
OpenSSH 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.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH Information Disclosure Vulnerability (CVE-2016-20012)(OID: 1.3.6.1.4.1.25623.1.0.117777)Version used: 2021-11-16T14:03:35Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.4Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://github.com/openssh/openssh-portable/pull/270,https://rushter.com/blog/public-ssh-keys/,https://utcc.utoronto.ca/~cks/space/blog/tech/SSHKeysAreInfoLeak

M

MEDIUM (CVSS: 5.3)

NVT: OPENSSH < 7.8 USER ENUMERATION VULNERABILITY - LINUX (OID: 1.3.6.1.4.1.25623.1.0.813864)

22/TCP (SSH)

Summary
OpenSSH is prone to a user enumeration vulnerability.

Vulnerability Detection Result
Installed version: 7.4Fixed version: 7.8Installationpath / port: 22/tcp

Impact
Successfully exploitation will allow remote attacker to test whether a certain user exists or not (username enumeration) on a target OpenSSH server.

Solution
Update to version 7.8 or later.

Vulnerability Insight
The flaw is due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH < 7.8 User Enumeration Vulnerability - Linux(OID: 1.3.6.1.4.1.25623.1.0.813864)Version used: 2021-10-11T09:46:29Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.4Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://0day.city/cve-2018-15473.html,https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a7d1e0

M

MEDIUM (CVSS: 5.3)

NVT: WEAK KEY EXCHANGE (KEX) ALGORITHM(S) SUPPORTED (SSH) (OID: 1.3.6.1.4.1.25623.1.0.150713)

22/TCP (SSH)

Summary
The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

Vulnerability Detection Result
The remote SSH server supports the following weak KEX algorithm(s):KEX algorithm | Reason---diffie-hellman-group-exchange-sha1 | Using SHA-1diffie-hellman-group1-sha1 | Using Oakley Group 2 (a 1024-bit MODP group) and SHA-1

Impact

An attacker can quickly break individual connections.

Solution
Disable the reported weak KEX algorithm(s) - 1024-bit MODP group / prime KEX algorithms: Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

Vulnerability Insight
'- 1024-bit MODP group / prime KEX algorithms: Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime. A nation-state can break a 1024-bit prime.

Vulnerability Detection Method
Checks the supported KEX algorithms of the remote SSH server. Currently weak KEX algorithms are defined as the following: - non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime - ephemerally generated key exchange groups uses SHA-1 - using RSA 1024-bit modulus keyDetails:Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)(OID: 1.3.6.1.4.1.25623.1.0.150713)Version used: 2021-11-24T06:31:19Z

References
https://weakdh.org/sysadmin.html,https://tools.ietf.org/id/draft-ietf-curdle-ssh-kex-sha2-09.html,https://tools.ietf.org/id/draft-ietf-curdle-ssh-kex-sha2-09.html#rfc.section.5,https://datatracker.ietf.org/doc/html/rfc6194

M

MEDIUM (CVSS: 5.3)

NVT: OPENSSH AUTH2-GSS.C USER ENUMERATION VULNERABILITY - LINUX (OID: 1.3.6.1.4.1.25623.1.0.813888)

22/TCP (SSH)

Summary
OpenSSH is prone to a user enumeration vulnerability.

Vulnerability Detection Result
Installed version: 7.4Fixed version: NoneInstallationpath / port: 22/tcp

Impact
Successfully exploitation will allow a remote attacker to harvest valid user accounts, which may aid in brute-force attacks.

Solution
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Vulnerability Insight
The flaw exists in the 'auth-gss2.c' source code file of the affected software and is due to insufficient validation of an authentication request packet when the Guide Star Server II (GSS2) component is used on an affected system.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH 'auth2-gss.c' User Enumeration Vulnerability - Linux(OID: 1.3.6.1.4.1.25623.1.0.813888)Version used: 2021-05-28T07:06:21Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.4Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://bugzilla.novell.com/show_bug.cgi?id=1106163,https://seclists.org/oss-sec/2018/q3/180

M

MEDIUM (CVSS: 4.3)

NVT: WEAK ENCRYPTION ALGORITHM(S) SUPPORTED (SSH) (OID: 1.3.6.1.4.1.25623.1.0.105611)

22/TCP (SSH)

Summary
The remote SSH server is configured to allow / support weak encryption algorithm(s).

Vulnerability Detection Result
The remote SSH server supports the following weak client-to-server encryption algorithm(s):3des-cbcaes128-cbcaes192-cbcaes256-cbcblowfish-cbccast128-cbcThe remote SSH server supports the following weak server-to-client encryption algorithm(s):3des-cbcaes128-cbcaes192-cbcaes256-cbcblowfish-cbccast128-cbc

Solution
Disable the reported weak encryption algorithm(s).

Vulnerability Insight
'- The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore. - The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it. - A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

Vulnerability Detection Method
Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server. Currently weak encryption algorithms are defined as the following: - Arcfour (RC4) cipher based algorithms - none algorithm - CBC mode cipher based algorithmsDetails:Weak Encryption Algorithm(s) Supported (SSH)(OID: 1.3.6.1.4.1.25623.1.0.105611)Version used: 2021-09-20T08:25:27Z

References
https://tools.ietf.org/html/rfc4253#section-6.3,https://www.kb.cert.org/vuls/id/958563

L

LOW (CVSS: 2.6)

NVT: TCP TIMESTAMPS (OID: 1.3.6.1.4.1.25623.1.0.80091)

0/NA

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
It was detected that the host implements RFC1323/RFC7323.The following timestamps were retrieved with a delay of 1 seconds in-between:Packet 1: 1180653861Packet 2: 1180654997

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.Details:TCP timestamps(OID: 1.3.6.1.4.1.25623.1.0.80091)Version used:

2020-08-24T08:40:10Z

References
http://www.ietf.org/rfc/rfc1323.txt,http://www.ietf.org/rfc/rfc7323.txt,https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152

2.4 - 176.16.1.64 (00:17:4G:01:07:C5)

Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	HIGHEST CVSS
176.16.1.64 (00:17:4G:01:07:C5)	2	2	1	1	7.5

Listening Ports

PORT
22/tcp (ssh), 0/NA

Security Issues

H

HIGH (CVSS: 7.5)

NVT: DIFFIE-HELLMAN EPHEMERAL KEY EXCHANGE DOS VULNERABILITY (SSH, D(HE)ATER) (OID: 1.3.6.1.4.1.25623.1.0.117839)

22/TCP (SSH)

Summary
The remote SSH server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange (KEX) algorithms and thus could be prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
The remote SSH server supports the following DHE KEX algorithm(s):diffie-hellman-group14-sha256diffie-hellman-group16-sha512diffie-hellman-group18-sha512diffie-hellman-group-exchange-sha256

Solution
'- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered. - Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For OpenSSH this limit can be configured via the 'MaxStartups' option, for other products please refer to the manual of the product in question on configuration possibilities.

Vulnerability Insight
The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE.

Vulnerability Detection Method
Checks the supported KEX algorithms of the remote SSH server.Details:Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSH, D(HE)ater)(OID: 1.3.6.1.4.1.25623.1.0.117839)Version used: 2021-12-17T14:03:21Z

References
https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Security_Issues_in_the_Diffie-Hellman_Key_Agreement_Protocol,https://github.com/Balasys/dheater

H

HIGH (CVSS: 7)

NVT: OPENSSH 6.2 <= 8.7 PRIVILEGE ESCALATION VULNERABILITY (OID: 1.3.6.1.4.1.25623.1.0.117696)

22/TCP (SSH)

Summary
OpenSSH is prone to a privilege scalation vulnerability in certain configurations.

Vulnerability Detection Result
Installed version: 8.4p1Fixed version: 8.8Installationpath / port: 22/tcp

Solution
Update to version 8.8 or later.

Vulnerability Insight
sshd failed to correctly initialise supplemental groups when executing an AuthorizedKeysCommand or AuthorizedPrincipalsCommand, where a AuthorizedKeysCommandUser or AuthorizedPrincipalsCommandUser directive has been set to run the command as a different user. Instead these commands would inherit the groups that sshd was started with. Depending on system configuration, inherited groups may allow AuthorizedKeysCommand/AuthorizedPrincipalsCommand helper programs to gain unintended privilege. Neither AuthorizedKeysCommand nor AuthorizedPrincipalsCommand are enabled by default in sshd_config.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH 6.2 <= 8.7 Privilege Escalation Vulnerability(OID: 1.3.6.1.4.1.25623.1.0.117696)Version used: 2021-10-11T08:01:31Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:8.4p1Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://www.openssh.com/txt/release-8.8

M

MEDIUM (CVSS: 5.3)

NVT: OPENSSH INFORMATION DISCLOSURE VULNERABILITY (CVE-2016-20012) (OID: 1.3.6.1.4.1.25623.1.0.117777)

22/TCP (SSH)

Summary
OpenBSD OpenSSH is prone to an information disclosure vulnerability.

Vulnerability Detection Result
Installed version: 8.4p1Fixed version: NoneInstallationpath / port: 22/tcp

Solution
No known solution is available as of 16th November, 2021. Information regarding this issue will be updated once solution details are available. Note: This issue is not treated as a security issue by the vendor so no update might be provided in the future.

Vulnerability Insight
OpenSSH 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.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH Information Disclosure Vulnerability (CVE-2016-20012)(OID: 1.3.6.1.4.1.25623.1.0.117777)Version used: 2021-11-16T14:03:35Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:8.4p1Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://github.com/openssh/openssh-portable/pull/270,https://rushter.com/blog/public-ssh-keys/,https://utcc.utoronto.ca/~cks/space/blog/tech/SSHKeysAreInfoLeak

L

LOW (CVSS: 2.6)
NVT: TCP TIMESTAMPS (OID: 1.3.6.1.4.1.25623.1.0.80091)

0/NA

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
It was detected that the host implements RFC1323/RFC7323.The following timestamps were retrieved with a delay of 1 seconds in-between:Packet 1: 3054012296Packet 2: 3054013448

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.Details:TCP timestamps(OID: 1.3.6.1.4.1.25623.1.0.80091)Version used: 2020-08-24T08:40:10Z

References
http://www.ietf.org/rfc/rfc1323.txt,http://www.ietf.org/rfc/rfc7323.txt,https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152

2.5 - 176.16.1.65 (00:17:4G:01:07:C6)

Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	HIGHEST CVSS
176.16.1.65 (00:17:4G:01:07:C6)	2	**2**	**1**	1	7.5

Listing Ports

PORT
22/tcp (ssh), 0/NA

Security Issues

H

HIGH (CVSS: 7.5)

NVT: DIFFIE-HELLMAN EPHEMERAL KEY EXCHANGE DOS VULNERABILITY (SSH, D(HE)ATER) (OID: 1.3.6.1.4.1.25623.1.0.117839)

22/TCP (SSH)

Summary
The remote SSH server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange (KEX) algorithms and thus could be prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
The remote SSH server supports the following DHE KEX algorithm(s):diffie-hellman-group14-sha256diffie-hellman-group16-sha512diffie-hellman-group18-sha512diffie-hellman-group-exchange-sha256

Solution
'- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered. - Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For OpenSSH this limit can be configured via the 'MaxStartups' option, for other products please refer to the manual of the product in question on configuration possibilities.

Vulnerability Insight
The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE.

Vulnerability Detection Method
Checks the supported KEX algorithms of the remote SSH server.Details:Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSH, D(HE)ater)(OID: 1.3.6.1.4.1.25623.1.0.117839)Version used: 2021-12-17T14:03:21Z

References
https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Security_Issues_in_the_Diffie-Hellman_Key_Agreement_Protocol,https://github.com/Balasys/dheater

H

HIGH (CVSS: 7)

NVT: OPENSSH 6.2 <= 8.7 PRIVILEGE ESCALATION VULNERABILITY (OID: 1.3.6.1.4.1.25623.1.0.117696)

22/TCP (SSH)

Summary
OpenSSH is prone to a privilege scalation vulnerability in certain configurations.

Vulnerability Detection Result

Installed version: 8.7Fixed version: 8.8Installationpath / port: 22/tcp

Solution
Update to version 8.8 or later.

Vulnerability Insight
sshd failed to correctly initialise supplemental groups when executing an AuthorizedKeysCommand or AuthorizedPrincipalsCommand, where a AuthorizedKeysCommandUser or AuthorizedPrincipalsCommandUser directive has been set to run the command as a different user. Instead these commands would inherit the groups that sshd was started with. Depending on system configuration, inherited groups may allow AuthorizedKeysCommand/AuthorizedPrincipalsCommand helper programs to gain unintended privilege. Neither AuthorizedKeysCommand nor AuthorizedPrincipalsCommand are enabled by default in sshd_config.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH 6.2 <= 8.7 Privilege Escalation Vulnerability(OID: 1.3.6.1.4.1.25623.1.0.117696)Version used: 2021-10-11T08:01:31Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:8.7Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://www.openssh.com/txt/release-8.8

M

MEDIUM (CVSS: 5.3)

NVT: OPENSSH INFORMATION DISCLOSURE VULNERABILITY (CVE-2016-20012) (OID: 1.3.6.1.4.1.25623.1.0.117777)

22/TCP (SSH)

Summary
OpenBSD OpenSSH is prone to an information disclosure vulnerability.

Vulnerability Detection Result
Installed version: 8.7Fixed version: NoneInstallationpath / port: 22/tcp

Solution
No known solution is available as of 16th November, 2021. Information regarding this issue will be updated once solution details are available. Note: This issue is not treated as a security issue by the vendor so no update might be provided in the future.

Vulnerability Insight
OpenSSH 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.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH Information Disclosure Vulnerability (CVE-2016-20012)(OID: 1.3.6.1.4.1.25623.1.0.117777)Version used: 2021-11-16T14:03:35Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:8.7Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://github.com/openssh/openssh-portable/pull/270,https://rushter.com/blog/public-ssh-keys/,https://utcc.utoronto.ca/~cks/space/blog/tech/SSHKeysAreInfoLeak

L

LOW (CVSS: 2.6)

NVT: TCP TIMESTAMPS (OID: 1.3.6.1.4.1.25623.1.0.80091)

0/NA

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
It was detected that the host implements RFC1323/RFC7323.The following timestamps were retrieved with a delay of 1 seconds in-between:Packet 1: 645972405Packet 2: 645973525

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.Details:TCP timestamps(OID: 1.3.6.1.4.1.25623.1.0.80091)Version used: 2020-08-24T08:40:10Z

References
http://www.ietf.org/rfc/rfc1323.txt,http://www.ietf.org/rfc/rfc7323.txt,https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152

2.6 - 176.16.1.67 (00:17:4G:01:07:C8)

Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	HIGHEST CVSS
176.16.1.67 (00:17:4G:01:07:C8)	2	2	4	1	7.5

Listening Ports

PORT
22/tcp (ssh), 0/NA

Security Issues

H

HIGH (CVSS: 7.5)

NVT: DIFFIE-HELLMAN EPHEMERAL KEY EXCHANGE DOS VULNERABILITY (SSH, D(HE)ATER) (OID: 1.3.6.1.4.1.25623.1.0.117839)

22/TCP (SSH)

Summary
The remote SSH server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange (KEX) algorithms and thus could be prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
The remote SSH server supports the following DHE KEX algorithm(s):diffie-hellman-group14-sha1diffie-hellman-group14-sha256diffie-hellman-group16-sha512diffie-hellman-group18-sha512diffie-hellman-group-exchange-sha1diffie-hellman-group-exchange-sha256

Solution
'- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered. - Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For OpenSSH this limit can be configured via the 'MaxStartups' option, for other products please refer to the manual of the product in question on configuration possibilities.

Vulnerability Insight
The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE.

Vulnerability Detection Method
Checks the supported KEX algorithms of the remote SSH server.Details:Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSH, D(HE)ater)(OID: 1.3.6.1.4.1.25623.1.0.117839)Version used: 2021-12-17T14:03:21Z

References
https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Security_Issues_in_the_Diffie-Hellman_Key_Agreement_Protocol,https://github.com/Balasys/dheater

HIGH (CVSS: 7)

NVT: OPENSSH 6.2 <= 8.7 PRIVILEGE ESCALATION VULNERABILITY (OID: 1.3.6.1.4.1.25623.1.0.117696)

22/TCP (SSH)

Summary
OpenSSH is prone to a privilege scalation vulnerability in certain configurations.

Vulnerability Detection Result
Installed version: 8.0Fixed version: 8.8Installationpath / port: 22/tcp

Solution
Update to version 8.8 or later.

Vulnerability Insight
sshd failed to correctly initialise supplemental groups when executing an AuthorizedKeysCommand or AuthorizedPrincipalsCommand, where a AuthorizedKeysCommandUser or AuthorizedPrincipalsCommandUser directive has been set to run the command as a different user. Instead these commands would inherit the groups that sshd was started with. Depending on system configuration, inherited groups may allow AuthorizedKeysCommand/AuthorizedPrincipalsCommand helper programs to gain unintended privilege. Neither AuthorizedKeysCommand nor AuthorizedPrincipalsCommand are enabled by default in sshd_config.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH 6.2 <= 8.7 Privilege Escalation Vulnerability(OID: 1.3.6.1.4.1.25623.1.0.117696)Version used: 2021-10-11T08:01:31Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:8.0Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://www.openssh.com/txt/release-8.8

M

MEDIUM (CVSS: 5.9)

NVT: OPENBSD OPENSSH INFORMATION DISCLOSURE VULNERABILITY (CVE-2020-14145) (OID: 1.3.6.1.4.1.25623.1.0.117785)

22/TCP (SSH)

Summary
OpenBSD OpenSSH is prone to an information disclosure vulnerability.

Vulnerability Detection Result
Installed version: 8.0Fixed version: 8.5Installationpath / port: 22/tcp

Solution
Update to version 8.5 or later.

Vulnerability Insight
The client side in OpenSSH 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).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenBSD OpenSSH Information Disclosure Vulnerability (CVE-2020-14145)(OID: 1.3.6.1.4.1.25623.1.0.117785)Version used: 2021-11-22T14:03:31Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:8.0Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
http://www.openwall.com/lists/oss-security/2020/12/02/1

M

MEDIUM (CVSS: 5.3)

NVT: WEAK KEY EXCHANGE (KEX) ALGORITHM(S) SUPPORTED (SSH) (OID: 1.3.6.1.4.1.25623.1.0.150713)

22/TCP (SSH)

Summary
The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

Vulnerability Detection Result
The remote SSH server supports the following weak KEX algorithm(s):KEX algorithm | Reason---diffie-hellman-group-exchange-sha1 | Using SHA-1

Impact
An attacker can quickly break individual connections.

Solution
Disable the reported weak KEX algorithm(s) - 1024-bit MODP group / prime KEX algorithms: Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

Vulnerability Insight
'- 1024-bit MODP group / prime KEX algorithms: Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime. A nation-state can break a 1024-bit prime.

Vulnerability Detection Method
Checks the supported KEX algorithms of the remote SSH server. Currently weak KEX algorithms are defined as the following: - non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime - ephemerally generated key exchange groups uses SHA-1 - using RSA 1024-bit modulus keyDetails:Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)(OID: 1.3.6.1.4.1.25623.1.0.150713)Version used: 2021-11-24T06:31:19Z

References
https://weakdh.org/sysadmin.html,https://tools.ietf.org/id/draft-ietf-curdle-ssh-kex-sha2-09.html,https://tools.ietf.org/id/draft-ietf-curdle-ssh-kex-sha2-09.html#rfc.section.5,https://datatracker.ietf.org/doc/html/rfc6194

MEDIUM (CVSS: 5.3)

NVT: OPENSSH INFORMATION DISCLOSURE VULNERABILITY (CVE-2016-20012) (OID: 1.3.6.1.4.1.25623.1.0.117777)

22/TCP (SSH)

Summary
OpenBSD OpenSSH is prone to an information disclosure vulnerability.

Vulnerability Detection Result
Installed version: 8.0Fixed version: NoneInstallationpath / port: 22/tcp

Solution
No known solution is available as of 16th November, 2021. Information regarding this issue will be updated once solution details are available. Note: This issue is not treated as a security issue by the vendor so no update might be provided in the future.

Vulnerability Insight
OpenSSH 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.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH Information Disclosure Vulnerability (CVE-2016-20012)(OID: 1.3.6.1.4.1.25623.1.0.117777)Version used: 2021-11-16T14:03:35Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:8.0Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://github.com/openssh/openssh-portable/pull/270,https://rushter.com/blog/public-ssh-keys/,https://utcc.utoronto.ca/~cks/space/blog/tech/SSHKeysAreInfoLeak

MEDIUM (CVSS: 4.3)

NVT: WEAK ENCRYPTION ALGORITHM(S) SUPPORTED (SSH) (OID: 1.3.6.1.4.1.25623.1.0.105611)

22/TCP (SSH)

Summary
The remote SSH server is configured to allow / support weak encryption algorithm(s).

Vulnerability Detection Result
The remote SSH server supports the following weak client-to-server encryption algorithm(s):aes128-cbcaes256-cbcThe remote SSH server supports the following weak server-to-client encryption algorithm(s):aes128-cbcaes256-cbc

Solution
Disable the reported weak encryption algorithm(s).

Vulnerability Insight

'- The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore. - The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it. - A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

Vulnerability Detection Method
Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server. Currently weak encryption algorithms are defined as the following: - Arcfour (RC4) cipher based algorithms - none algorithm - CBC mode cipher based algorithmsDetails:Weak Encryption Algorithm(s) Supported (SSH)(OID: 1.3.6.1.4.1.25623.1.0.105611)Version used: 2021-09-20T08:25:27Z

References
https://tools.ietf.org/html/rfc4253#section-6.3,https://www.kb.cert.org/vuls/id/958563

L

LOW (CVSS: 2.6)
NVT: TCP TIMESTAMPS (OID: 1.3.6.1.4.1.25623.1.0.80091)

0/NA

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
It was detected that the host implements RFC1323/RFC7323.The following timestamps were retrieved with a delay of 1 seconds in-between:Packet 1: 2892023837Packet 2: 2892024949

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.Details:TCP timestamps(OID: 1.3.6.1.4.1.25623.1.0.80091)Version used: 2020-08-24T08:40:10Z

References
http://www.ietf.org/rfc/rfc1323.txt,http://www.ietf.org/rfc/rfc7323.txt,https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152

2.7 - 176.16.1.70 (B0:26:28:B6:DC:4F)

Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	HIGHEST CVSS
176.16.1.70 (B0:26:28:B6:DC:4F)	1	**1**	**1**	0	7.5

Listening Ports

PORT
3389/tcp

Security Issues

H

HIGH (CVSS: 7.5)

NVT: DIFFIE-HELLMAN EPHEMERAL KEY EXCHANGE DOS VULNERABILITY (SSL/TLS, D(HE)ATER) (OID: 1.3.6.1.4.1.25623.1.0.117840)

3389/TCP

Summary
The remote SSL/TLS server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange algorithms and thus could be prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
'DHE' cipher suites accepted by this service via the TLSv1.2 protocol:TLS_DHE_RSA_WITH_AES_128_GCM_SHA256TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Solution
'- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered. - Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For Postfix this limit can be configured via 'smtpd_client_new_tls_session_rate_limit' option, for other products please refer to the manual of the product in question on configuration possibilities.

Vulnerability Insight
The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE.

Vulnerability Detection Method
Checks the supported cipher suites of the remote SSL/TLS server.Details:Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater)(OID: 1.3.6.1.4.1.25623.1.0.117840)Version used: 2021-12-17T14:03:21Z

References
https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Security_Issues_in_the_Diffie-Hellman_Key_Agreement_Protocol,https://github.com/Balasys/dheater

M

MEDIUM (CVSS: 4.3)

NVT: SSL/TLS: DEPRECATED TLSV1.0 AND TLSV1.1 PROTOCOL DETECTION (OID: 1.3.6.1.4.1.25623.1.0.117274)

3389/TCP

Summary
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Vulnerability Detection Result
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.

Impact
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Vulnerability Insight
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like: - CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST) - CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method
Check the used TLS protocols of the services provided by this system.Details:SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection(OID: 1.3.6.1.4.1.25623.1.0.117274)Version used: 2021-07-19T08:11:48Z

References
https://ssl-config.mozilla.org/,https://bettercrypto.org/,https://datatracker.ietf.org/doc/rfc8996/,https://vnhacker.blogspot.com/2011/09/beast.html,https://web.archive.org/web/20201108095603/https://censys.io/blog/freak,https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014

2.8 - deskpc-0o3l5bq.myco.com (176.16.1.73 / 00:17:4G:01:08:38)

Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	HIGHEST CVSS
deskpc-0o3l5bq.myco.com (176.16.1.73 / 00:17:4G:01:08:38)	1	**1**	**1**	0	7.5

Listening Ports

PORT
3389/tcp

Security Issues

H

HIGH (CVSS: 7.5)

NVT: DIFFIE-HELLMAN EPHEMERAL KEY EXCHANGE DOS VULNERABILITY (SSL/TLS, D(HE)ATER) (OID: 1.3.6.1.4.1.25623.1.0.117840)

3389/TCP

Summary
The remote SSL/TLS server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange algorithms and thus could be prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
'DHE' cipher suites accepted by this service via the TLSv1.2 protocol:TLS_DHE_RSA_WITH_AES_128_GCM_SHA256TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Solution
'- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered. - Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For Postfix this limit can be configured via 'smtpd_client_new_tls_session_rate_limit' option, for other products please refer to the manual of the product in question on configuration possibilities.

Vulnerability Insight
The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE.

Vulnerability Detection Method
Checks the supported cipher suites of the remote SSL/TLS server.Details:Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater)(OID: 1.3.6.1.4.1.25623.1.0.117840)Version used: 2021-12-17T14:03:21Z

References
https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Security_Issues_in_the_Diffie-Hellman_Key_Agreement_Protocol,https://github.com/Balasys/dheater

M

MEDIUM (CVSS: 4.3)

NVT: SSL/TLS: DEPRECATED TLSV1.0 AND TLSV1.1 PROTOCOL DETECTION (OID: 1.3.6.1.4.1.25623.1.0.117274)

3389/TCP

Summary
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Vulnerability Detection Result
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.

Impact
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Vulnerability Insight

The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like: - CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST) - CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method
Check the used TLS protocols of the services provided by this system.Details:SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection(OID: 1.3.6.1.4.1.25623.1.0.117274)Version used: 2021-07-19T08:11:48Z

References
https://ssl-config.mozilla.org/,https://bettercrypto.org/,https://datatracker.ietf.org/doc/rfc8996/,https://vnhacker.blogspot.com/2011/09/beast.html,https://web.archive.org/web/20201108095603/https://censys.io/blog/freak,https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014

2.9 - sql03.myco.com (176.16.1.107 / 00:17:4G:01:07:32)

Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	HIGHEST CVSS
sql03.myco.com (176.16.1.107 / 00:17:4G:01:07:32)	1	1	0	0	7.5

Listening Ports

PORT
3389/tcp

Security Issues

H	HIGH (CVSS: 7.5) NVT: DIFFIE-HELLMAN EPHEMERAL KEY EXCHANGE DOS VULNERABILITY (SSL/TLS, D(HE)ATER) (OID: 1.3.6.1.4.1.25623.1.0.117840)	3389/TCP

Summary
The remote SSL/TLS server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange algorithms and thus could be prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
'DHE' cipher suites accepted by this service via the TLSv1.2 protocol:TLS_DHE_RSA_WITH_AES_128_GCM_SHA256TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Solution
'- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret

should be considered. - Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For Postfix this limit can be configured via 'smtpd_client_new_tls_session_rate_limit' option, for other products please refer to the manual of the product in question on configuration possibilities.

Vulnerability Insight
The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE.

Vulnerability Detection Method
Checks the supported cipher suites of the remote SSL/TLS server.Details:Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater)(OID: 1.3.6.1.4.1.25623.1.0.117840)Version used: 2021-12-17T14:03:21Z

References
https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Security_Issues_in_the_Diffie-Hellman_Key_Agreement_Protocol,https://github.com/Balasys/dheater

2.10 - 176.16.1.147 (B0:26:28:B6:C6:4C)

Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	HIGHEST CVSS
176.16.1.147 (B0:26:28:B6:C6:4C)	1	1	0	0	7.5

Listening Ports

PORT
3389/tcp

Security Issues

H

HIGH (CVSS: 7.5)

NVT: DIFFIE-HELLMAN EPHEMERAL KEY EXCHANGE DOS VULNERABILITY (SSL/TLS, D(HE)ATER) (OID: 1.3.6.1.4.1.25623.1.0.117840)

3389/TCP

Summary
The remote SSL/TLS server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange algorithms and thus could be prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
'DHE' cipher suites accepted by this service via the TLSv1.2 protocol:TLS_DHE_RSA_WITH_AES_128_GCM_SHA256TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Solution

'- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered. - Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For Postfix this limit can be configured via 'smtpd_client_new_tls_session_rate_limit' option, for other products please refer to the manual of the product in question on configuration possibilities.

Vulnerability Insight
The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE.

Vulnerability Detection Method
Checks the supported cipher suites of the remote SSL/TLS server.Details:Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater)(OID: 1.3.6.1.4.1.25623.1.0.117840)Version used: 2021-12-17T14:03:21Z

References
https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Security_Issues_in_the_Diffie-Hellman_Key_Agreement_Protocol,https://github.com/Balasys/dheater

2.11 - 176.16.1.148 (B0:26:28:B6:DC:4E)

Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	HIGHEST CVSS
176.16.1.148 (B0:26:28:B6:DC:4E)	1	1	0	0	7.5

Listening Ports

PORT
3389/tcp

Security Issues

H

HIGH (CVSS: 7.5)

NVT: DIFFIE-HELLMAN EPHEMERAL KEY EXCHANGE DOS VULNERABILITY (SSL/TLS, D(HE)ATER) (OID: 1.3.6.1.4.1.25623.1.0.117840)

3389/TCP

Summary
The remote SSL/TLS server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange algorithms and thus could be prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
'DHE' cipher suites accepted by this service via the TLSv1.2 protocol:TLS_DHE_RSA_WITH_AES_128_GCM_SHA256TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Solution
'- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered. - Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For Postfix this limit can be configured via 'smtpd_client_new_tls_session_rate_limit' option, for other products please refer to the manual of the product in question on configuration possibilities.

Vulnerability Insight
The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE.

Vulnerability Detection Method
Checks the supported cipher suites of the remote SSL/TLS server.Details:Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater)(OID: 1.3.6.1.4.1.25623.1.0.117840)Version used: 2021-12-17T14:03:21Z

References
https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Security_Issues_in_the_Diffie-Hellman_Key_Agreement_Protocol,https://github.com/Balasys/dheater

2.12 - 176.16.1.156 (00:17:4G:01:07:7B)

Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	HIGHEST CVSS
176.16.1.156 (00:17:4G:01:07:7B)	2	2	7	1	7.5

Listening Ports

PORT
22/tcp (ssh), 0/NA

Security Issues

H

HIGH (CVSS: 7.5)

NVT: DIFFIE-HELLMAN EPHEMERAL KEY EXCHANGE DOS VULNERABILITY (SSH, D(HE)ATER) (OID: 1.3.6.1.4.1.25623.1.0.117839)

22/TCP (SSH)

Summary
The remote SSH server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange (KEX) algorithms and thus could be prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
The remote SSH server supports the following DHE KEX algorithm(s):diffie-hellman-group1-sha1diffie-hellman-group14-

sha1diffie-hellman-group14-sha256diffie-hellman-group16-sha512diffie-hellman-group18-sha512diffie-hellman-group-exchange-sha1diffie-hellman-group-exchange-sha256

Solution
'- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered. - Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For OpenSSH this limit can be configured via the 'MaxStartups' option, for other products please refer to the manual of the product in question on configuration possibilities.

Vulnerability Insight
The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE.

Vulnerability Detection Method
Checks the supported KEX algorithms of the remote SSH server.Details:Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSH, D(HE)ater)(OID: 1.3.6.1.4.1.25623.1.0.117839)Version used: 2021-12-17T14:03:21Z

References
https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Security_Issues_in_the_Diffie-Hellman_Key_Agreement_Protocol,https://github.com/Balasys/dheater

H

HIGH (CVSS: 7)

NVT: OPENSSH 6.2 <= 8.7 PRIVILEGE ESCALATION VULNERABILITY (OID: 1.3.6.1.4.1.25623.1.0.117696)

22/TCP (SSH)

Summary
OpenSSH is prone to a privilege scalation vulnerability in certain configurations.

Vulnerability Detection Result
Installed version: 7.4Fixed version: 8.8Installationpath / port: 22/tcp

Solution
Update to version 8.8 or later.

Vulnerability Insight
sshd failed to correctly initialise supplemental groups when executing an AuthorizedKeysCommand or AuthorizedPrincipalsCommand, where a AuthorizedKeysCommandUser or AuthorizedPrincipalsCommandUser directive has been set to run the command as a different user. Instead these commands would inherit the groups that sshd was started with. Depending on system configuration, inherited groups may allow AuthorizedKeysCommand/AuthorizedPrincipalsCommand helper programs to gain unintended privilege. Neither AuthorizedKeysCommand nor AuthorizedPrincipalsCommand are enabled by default in sshd_config.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH 6.2 <= 8.7 Privilege Escalation Vulnerability(OID: 1.3.6.1.4.1.25623.1.0.117696)Version used: 2021-10-11T08:01:31Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.4Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://www.openssh.com/txt/release-8.8

M

MEDIUM (CVSS: 5.9)

NVT: OPENBSD OPENSSH <= 7.9 MULTIPLE VULNERABILITIES (OID: 1.3.6.1.4.1.25623.1.0.117786)

22/TCP (SSH)

Summary
OpenBSD OpenSSH is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 7.4Fixed version: 8.0Installationpath / port: 22/tcp

Solution
Update to version 8.0 or later.

Vulnerability Insight
The following flaws exist: - CVE-2018-20685: bypass of intended access restrictions in the scp client - CVE-2019-6109, CVE-2019-6110: manipulation of the output in the scp client by a malicious server - CVE-2019-6111: overwrite of arbitrary files in the scp client by a malicious server

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenBSD OpenSSH <= 7.9 Multiple Vulnerabilities(OID: 1.3.6.1.4.1.25623.1.0.117786)Version used: 2021-11-22T14:03:31Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.4Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://sintonen.fi/advisories/scp-client-multiple-vulnerabilities.txt,http://www.openwall.com/lists/oss-security/2019/04/18/1

M

MEDIUM (CVSS: 5.9)

NVT: OPENBSD OPENSSH INFORMATION DISCLOSURE VULNERABILITY (CVE-2020-14145) (OID: 1.3.6.1.4.1.25623.1.0.117785)

22/TCP (SSH)

Summary
OpenBSD OpenSSH is prone to an information disclosure vulnerability.

Vulnerability Detection Result
Installed version: 7.4Fixed version: 8.5Installationpath / port: 22/tcp

Solution
Update to version 8.5 or later.

Vulnerability Insight
The client side in OpenSSH 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).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenBSD OpenSSH Information Disclosure Vulnerability (CVE-2020-14145)(OID: 1.3.6.1.4.1.25623.1.0.117785)Version used: 2021-11-22T14:03:31Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.4Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
http://www.openwall.com/lists/oss-security/2020/12/02/1

MEDIUM (CVSS: 5.3)

NVT: OPENSSH < 7.8 USER ENUMERATION VULNERABILITY - LINUX (OID: 1.3.6.1.4.1.25623.1.0.813864)

22/TCP (SSH)

Summary
OpenSSH is prone to a user enumeration vulnerability.

Vulnerability Detection Result
Installed version: 7.4Fixed version: 7.8Installationpath / port: 22/tcp

Impact
Successfully exploitation will allow remote attacker to test whether a certain user exists or not (username enumeration) on a target OpenSSH server.

Solution
Update to version 7.8 or later.

Vulnerability Insight
The flaw is due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH < 7.8 User Enumeration Vulnerability - Linux(OID: 1.3.6.1.4.1.25623.1.0.813864)Version used: 2021-10-11T09:46:29Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.4Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://0day.city/cve-2018-15473.html,https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a7d1e0

MEDIUM (CVSS: 5.3)

NVT: OPENSSH SFTP-SERVER SECURITY BYPASS VULNERABILITY (LINUX) (OID: 1.3.6.1.4.1.25623.1.0.812051)

22/TCP (SSH)

Summary
openssh is prone to a security bypass vulnerability.

Vulnerability Detection Result
Installed version: 7.4Fixed version: 7.6Installationpath / port: 22/tcp

Impact
Successfully exploiting this issue allows local users to bypass certain security restrictions and perform unauthorized actions. This may lead to further attacks.

Solution
Upgrade to OpenSSH version 7.6 or later.

Vulnerability Insight
The flaw exists in the 'process_open' function in sftp-server.c script which does not properly prevent write operations in readonly mode.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH 'sftp-server' Security Bypass Vulnerability (Linux)(OID: 1.3.6.1.4.1.25623.1.0.812051)Version used: 2022-04-13T11:57:07Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.4Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://www.openssh.com/txt/release-7.6,https://github.com/openbsd/src/commit/a6981567e8e

M

MEDIUM (CVSS: 5.3)

NVT: WEAK KEY EXCHANGE (KEX) ALGORITHM(S) SUPPORTED (SSH) (OID: 1.3.6.1.4.1.25623.1.0.150713)

22/TCP (SSH)

Summary
The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

Vulnerability Detection Result
The remote SSH server supports the following weak KEX algorithm(s):KEX algorithm | Reason---diffie-hellman-group-exchange-sha1 | Using SHA-1diffie-hellman-group1-sha1 | Using Oakley Group 2 (a 1024-bit MODP group) and SHA-1

Impact
An attacker can quickly break individual connections.

Solution
Disable the reported weak KEX algorithm(s) - 1024-bit MODP group / prime KEX algorithms: Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

Vulnerability Insight
'- 1024-bit MODP group / prime KEX algorithms: Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime. A nation-state can break a 1024-bit prime.

Vulnerability Detection Method
Checks the supported KEX algorithms of the remote SSH server. Currently weak KEX algorithms are defined as the following: - non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime - ephemerally generated key exchange groups uses SHA-1 - using RSA 1024-bit modulus keyDetails:Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)(OID: 1.3.6.1.4.1.25623.1.0.150713)Version used: 2021-11-24T06:31:19Z

References
https://weakdh.org/sysadmin.html,https://tools.ietf.org/id/draft-ietf-curdle-ssh-kex-sha2-09.html,https://tools.ietf.org/id/draft-ietf-curdle-ssh-kex-sha2-09.html#rfc.section.5,https://datatracker.ietf.org/doc/html/rfc6194

M

MEDIUM (CVSS: 5.3)

NVT: OPENSSH AUTH2-GSS.C USER ENUMERATION VULNERABILITY - LINUX (OID: 1.3.6.1.4.1.25623.1.0.813888)

22/TCP (SSH)

Summary
OpenSSH is prone to a user enumeration vulnerability.

Vulnerability Detection Result
Installed version: 7.4Fixed version: NoneInstallationpath / port: 22/tcp

Impact
Successfully exploitation will allow a remote attacker to harvest valid user accounts, which may aid in brute-force attacks.

Solution

No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Vulnerability Insight
The flaw exists in the 'auth-gss2.c' source code file of the affected software and is due to insufficient validation of an authentication request packet when the Guide Star Server II (GSS2) component is used on an affected system.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH 'auth2-gss.c' User Enumeration Vulnerability - Linux(OID: 1.3.6.1.4.1.25623.1.0.813888)Version used: 2021-05-28T07:06:21Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.4Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://bugzilla.novell.com/show_bug.cgi?id=1106163,https://seclists.org/oss-sec/2018/q3/180

M

MEDIUM (CVSS: 5.3)

NVT: OPENSSH INFORMATION DISCLOSURE VULNERABILITY (CVE-2016-20012) (OID: 1.3.6.1.4.1.25623.1.0.117777)

22/TCP (SSH)

Summary
OpenBSD OpenSSH is prone to an information disclosure vulnerability.

Vulnerability Detection Result
Installed version: 7.4Fixed version: NoneInstallationpath / port: 22/tcp

Solution
No known solution is available as of 16th November, 2021. Information regarding this issue will be updated once solution details are available. Note: This issue is not treated as a security issue by the vendor so no update might be provided in the future.

Vulnerability Insight
OpenSSH 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.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH Information Disclosure Vulnerability (CVE-2016-20012)(OID: 1.3.6.1.4.1.25623.1.0.117777)Version used: 2021-11-16T14:03:35Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.4Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://github.com/openssh/openssh-portable/pull/270,https://rushter.com/blog/public-ssh-keys/,https://utcc.utoronto.ca/~cks/space/blog/tech/SSHKeysAreInfoLeak

L

LOW (CVSS: 2.6)

NVT: TCP TIMESTAMPS (OID: 1.3.6.1.4.1.25623.1.0.80091)

0/NA

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result

It was detected that the host implements RFC1323/RFC7323.The following timestamps were retrieved with a delay of 1 seconds in-between:Packet 1: 1027203671Packet 2: 1027204815

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.Details:TCP timestamps(OID: 1.3.6.1.4.1.25623.1.0.80091)Version used: 2020-08-24T08:40:10Z

References
http://www.ietf.org/rfc/rfc1323.txt,http://www.ietf.org/rfc/rfc7323.txt,https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152

2.13 - deskpc-f6ckerq.myco.com (176.16.1.171 / 00:17:4G:01:08:02)

Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	HIGHEST CVSS
deskpc-f6ckerq.myco.com (176.16.1.171 / 00:17:4G:01:08:02)	1	1	0	0	7.5

Listening Ports

PORT
3389/tcp

Security Issues

H

HIGH (CVSS: 7.5)

NVT: DIFFIE-HELLMAN EPHEMERAL KEY EXCHANGE DOS VULNERABILITY (SSL/TLS, D(HE)ATER) (OID: 1.3.6.1.4.1.25623.1.0.117840)

3389/TCP

Summary
The remote SSL/TLS server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange algorithms and thus could be prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
'DHE' cipher suites accepted by this service via the TLSv1.2 protocol:TLS_DHE_RSA_WITH_AES_128_GCM_SHA256TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Solution
'- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered. - Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For Postfix this limit can be configured via 'smtpd_client_new_tls_session_rate_limit' option, for other products please refer to the manual of the product in question on configuration possibilities.

Vulnerability Insight
The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE.

Vulnerability Detection Method
Checks the supported cipher suites of the remote SSL/TLS server.Details:Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater)(OID: 1.3.6.1.4.1.25623.1.0.117840)Version used: 2021-12-17T14:03:21Z

References
https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Security_Issues_in_the_Diffie-Hellman_Key_Agreement_Protocol,https://github.com/Balasys/dheater

2.14 - 176.16.1.178 (00:17:4G:01:07:94)

Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	HIGHEST CVSS
176.16.1.178 (00:17:4G:01:07:94)	2	2	1	1	7.5

Listening Ports

PORT
22/tcp (ssh), 0/NA

Security Issues

H	HIGH (CVSS: 7.5) NVT: DIFFIE-HELLMAN EPHEMERAL KEY EXCHANGE DOS VULNERABILITY (SSH, D(HE)ATER) (OID: 1.3.6.1.4.1.25623.1.0.117839)	22/TCP (SSH)

Summary
The remote SSH server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange (KEX) algorithms and thus could be prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
The remote SSH server supports the following DHE KEX algorithm(s):diffie-hellman-group14-sha256diffie-hellman-group16-sha512diffie-hellman-group18-sha512diffie-hellman-group-exchange-sha256

Solution
'- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered. - Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For OpenSSH this limit can be configured via the 'MaxStartups' option, for other products please refer to the manual of the product in question on configuration possibilities.

Vulnerability Insight
The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE.

Vulnerability Detection Method
Checks the supported KEX algorithms of the remote SSH server.Details:Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSH, D(HE)ater)(OID: 1.3.6.1.4.1.25623.1.0.117839)Version used: 2021-12-17T14:03:21Z

References
https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Security_Issues_in_the_Diffie-Hellman_Key_Agreement_Protocol,https://github.com/Balasys/dheater

H	HIGH (CVSS: 7) NVT: OPENSSH 6.2 <= 8.7 PRIVILEGE ESCALATION VULNERABILITY (OID: 1.3.6.1.4.1.25623.1.0.117696)	22/TCP (SSH)

Summary
OpenSSH is prone to a privilege scalation vulnerability in certain configurations.

Vulnerability Detection Result
Installed version: 8.6Fixed version: 8.8Installationpath / port: 22/tcp

Solution
Update to version 8.8 or later.

Vulnerability Insight
sshd failed to correctly initialise supplemental groups when executing an AuthorizedKeysCommand or AuthorizedPrincipalsCommand, where a AuthorizedKeysCommandUser or AuthorizedPrincipalsCommandUser directive has been set to run the command as a different user. Instead these commands would inherit the groups that sshd was started with. Depending on system configuration, inherited groups may allow AuthorizedKeysCommand/AuthorizedPrincipalsCommand helper programs to gain unintended privilege. Neither AuthorizedKeysCommand nor AuthorizedPrincipalsCommand are enabled by default in sshd_config.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH 6.2 <= 8.7 Privilege Escalation Vulnerability(OID: 1.3.6.1.4.1.25623.1.0.117696)Version used: 2021-10-11T08:01:31Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:8.6Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://www.openssh.com/txt/release-8.8

M

MEDIUM (CVSS: 5.3)

NVT: OPENSSH INFORMATION DISCLOSURE VULNERABILITY (CVE-2016-20012) (OID: 1.3.6.1.4.1.25623.1.0.117777)

22/TCP (SSH)

Summary
OpenBSD OpenSSH is prone to an information disclosure vulnerability.

Vulnerability Detection Result
Installed version: 8.6Fixed version: NoneInstallationpath / port: 22/tcp

Solution
No known solution is available as of 16th November, 2021. Information regarding this issue will be updated once solution details are available. Note: This issue is not treated as a security issue by the vendor so no update might be provided in the future.

Vulnerability Insight
OpenSSH 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.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH Information Disclosure Vulnerability (CVE-2016-20012)(OID: 1.3.6.1.4.1.25623.1.0.117777)Version used: 2021-11-16T14:03:35Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:8.6Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://github.com/openssh/openssh-portable/pull/270,https://rushter.com/blog/public-ssh-keys/,https://utcc.utoronto.ca/~cks/space/blog/tech/SSHKeysAreInfoLeak

L

LOW (CVSS: 2.6)

NVT: TCP TIMESTAMPS (OID: 1.3.6.1.4.1.25623.1.0.80091)

0/NA

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
It was detected that the host implements RFC1323/RFC7323.The following timestamps were retrieved with a delay of 1 seconds in-between:Packet 1: 2560593265Packet 2: 2560594370

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.Details:TCP timestamps(OID: 1.3.6.1.4.1.25623.1.0.80091)Version used: 2020-08-24T08:40:10Z

References
http://www.ietf.org/rfc/rfc1323.txt,http://www.ietf.org/rfc/rfc7323.txt,https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152

2.15 - winpc-tatvq3rem1k.myco.com (176.16.1.211 / 00:17:4G:01:07:B3)

Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	HIGHEST CVSS
winpc-tatvq3rem1k.myco.com (176.16.1.211 / 00:17:4G:01:07:B3)	1	1	1	0	7.5

Listening Ports

PORT
3389/tcp

Security Issues

H	HIGH (CVSS: 7.5) NVT: DIFFIE-HELLMAN EPHEMERAL KEY EXCHANGE DOS VULNERABILITY (SSL/TLS, D(HE)ATER) (OID: 1.3.6.1.4.1.25623.1.0.117840)	3389/TCP

Summary
The remote SSL/TLS server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange algorithms and thus could be prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
'DHE' cipher suites accepted by this service via the TLSv1.2 protocol:TLS_DHE_RSA_WITH_AES_128_GCM_SHA256TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Solution
'- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered. - Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For Postfix this limit can be configured via 'smtpd_client_new_tls_session_rate_limit' option, for other products please refer to the manual of the product in question on configuration possibilities.

Vulnerability Insight

The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE.

Vulnerability Detection Method
Checks the supported cipher suites of the remote SSL/TLS server.Details:Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater)(OID: 1.3.6.1.4.1.25623.1.0.117840)Version used: 2021-12-17T14:03:21Z

References
https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Security_Issues_in_the_Diffie-Hellman_Key_Agreement_Protocol,https://github.com/Balasys/dheater

M

MEDIUM (CVSS: 4.3)

NVT: SSL/TLS: DEPRECATED TLSV1.0 AND TLSV1.1 PROTOCOL DETECTION (OID: 1.3.6.1.4.1.25623.1.0.117274)

3389/TCP

Summary
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Vulnerability Detection Result
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.

Impact
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Vulnerability Insight
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like: - CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST) - CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method
Check the used TLS protocols of the services provided by this system.Details:SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection(OID: 1.3.6.1.4.1.25623.1.0.117274)Version used: 2021-07-19T08:11:48Z

References
https://ssl-config.mozilla.org/,https://bettercrypto.org/,https://datatracker.ietf.org/doc/rfc8996/,https://vnhacker.blogspot.com/2011/09/beast.html,https://web.archive.org/web/20201108095603/https://censys.io/blog/freak,https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014

2.16 - deskpc-07rd86g.myco.com (176.16.1.213 / 00:17:4G:01:08:31)

Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	HIGHEST CVSS
deskpc-07rd86g.myco.com (176.16.1.213 / 00:17:4G:01:08:31)	1	1	1	0	7.5

Listing Ports

PORT
3389/tcp

Security Issues

H

HIGH (CVSS: 7.5)

NVT: DIFFIE-HELLMAN EPHEMERAL KEY EXCHANGE DOS VULNERABILITY (SSL/TLS, D(HE)ATER) (OID: 1.3.6.1.4.1.25623.1.0.117840)

3389/TCP

Summary
The remote SSL/TLS server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange algorithms and thus could be prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
'DHE' cipher suites accepted by this service via the TLSv1.2 protocol:TLS_DHE_RSA_WITH_AES_128_GCM_SHA256TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Solution
'- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered. - Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For Postfix this limit can be configured via 'smtpd_client_new_tls_session_rate_limit' option, for other products please refer to the manual of the product in question on configuration possibilities.

Vulnerability Insight
The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE.

Vulnerability Detection Method
Checks the supported cipher suites of the remote SSL/TLS server.Details:Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater)(OID: 1.3.6.1.4.1.25623.1.0.117840)Version used: 2021-12-17T14:03:21Z

References
https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Security_Issues_in_the_Diffie-Hellman_Key_Agreement_Protocol,https://github.com/Balasys/dheater

M

MEDIUM (CVSS: 4.3)

NVT: SSL/TLS: DEPRECATED TLSV1.0 AND TLSV1.1 PROTOCOL DETECTION (OID: 1.3.6.1.4.1.25623.1.0.117274)

3389/TCP

Summary
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Vulnerability Detection Result
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.

Impact
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Vulnerability Insight
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like: - CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST) - CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method
Check the used TLS protocols of the services provided by this system.Details:SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection(OID: 1.3.6.1.4.1.25623.1.0.117274)Version used: 2021-07-19T08:11:48Z

References
https://ssl-config.mozilla.org/,https://bettercrypto.org/,https://datatracker.ietf.org/doc/rfc8996/,https://vnhacker.blogspot.com/2011/09/beast.html,https://web.archive.org/web/20201108095603/https://censys.io/blog/freak,https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014

2.17 - 176.16.1.219 (00:17:4G:01:08:32)

Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	HIGHEST CVSS
176.16.1.219 (00:17:4G:01:08:32)	1	3	2	0	7.5

Listening Ports

PORT
22/tcp (ssh)

Security Issues

H	HIGH (CVSS: 7.5) NVT: DIFFIE-HELLMAN EPHEMERAL KEY EXCHANGE DOS VULNERABILITY (SSH, D(HE)ATER) (OID: 1.3.6.1.4.1.25623.1.0.117839)	22/TCP (SSH)

Summary
The remote SSH server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange (KEX) algorithms and thus could be prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
The remote SSH server supports the following DHE KEX algorithm(s):diffie-hellman-group14-sha256diffie-hellman-group16-sha512diffie-hellman-group18-sha512diffie-hellman-group-exchange-sha256

Solution
'- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered. - Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For OpenSSH this limit can be configured via the 'MaxStartups' option, for other products please refer to the manual of the product in question on configuration possibilities.

Vulnerability Insight
The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE.

Vulnerability Detection Method
Checks the supported KEX algorithms of the remote SSH server.Details:Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSH, D(HE)ater)(OID: 1.3.6.1.4.1.25623.1.0.117839)Version used: 2021-12-17T14:03:21Z

References
https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Security_Issues_in_the_Diffie-Hellman_Key_Agreement_Protocol,https://github.com/Balasys/dheater

H	HIGH (CVSS: 7.1) NVT: OPENSSH 8.2 < 8.5 MEMORY CORRUPTION VULNERABILITY (OID: 1.3.6.1.4.1.25623.1.0.145538)	22/TCP (SSH)

Summary
OpenSSH is prone to a memory corruption vulnerability in the ssh-agent.

Vulnerability Detection Result
Installed version: 8.2p1Fixed version: 8.5Installationpath / port: 22/tcp

Solution
Update to version 8.5 or later.

Vulnerability Insight
ssh-agent in OpenSSH 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.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.Details:OpenSSH 8.2 < 8.5 Memory Corruption Vulnerability(OID: 1.3.6.1.4.1.25623.1.0.145538)Version used: 2021-08-17T12:00:57Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:8.2p1Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://www.openssh.com/txt/release-8.5

H

HIGH (CVSS: 7)

NVT: OPENSSH 6.2 <= 8.7 PRIVILEGE ESCALATION VULNERABILITY (OID: 1.3.6.1.4.1.25623.1.0.117696)

22/TCP
(SSH)

Summary
OpenSSH is prone to a privilege scalation vulnerability in certain configurations.

Vulnerability Detection Result
Installed version: 8.2p1Fixed version: 8.8Installationpath / port: 22/tcp

Solution
Update to version 8.8 or later.

Vulnerability Insight
sshd failed to correctly initialise supplemental groups when executing an AuthorizedKeysCommand or AuthorizedPrincipalsCommand, where a AuthorizedKeysCommandUser or AuthorizedPrincipalsCommandUser directive has been set to run the command as a different user. Instead these commands would inherit the groups that sshd was started with. Depending on system configuration, inherited groups may allow AuthorizedKeysCommand/AuthorizedPrincipalsCommand helper programs to gain unintended privilege. Neither AuthorizedKeysCommand nor AuthorizedPrincipalsCommand are enabled by default in sshd_config.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH 6.2 <= 8.7 Privilege Escalation Vulnerability(OID: 1.3.6.1.4.1.25623.1.0.117696)Version used: 2021-10-11T08:01:31Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:8.2p1Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://www.openssh.com/txt/release-8.8

M

MEDIUM (CVSS: 5.9)

NVT: OPENBSD OPENSSH INFORMATION DISCLOSURE VULNERABILITY (CVE-2020-14145) (OID: 1.3.6.1.4.1.25623.1.0.117785)

22/TCP
(SSH)

Summary
OpenBSD OpenSSH is prone to an information disclosure vulnerability.

Vulnerability Detection Result
Installed version: 8.2p1Fixed version: 8.5Installationpath / port: 22/tcp

Solution
Update to version 8.5 or later.

Vulnerability Insight
The client side in OpenSSH 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).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenBSD OpenSSH Information Disclosure Vulnerability (CVE-2020-14145)(OID: 1.3.6.1.4.1.25623.1.0.117785)Version used: 2021-11-22T14:03:31Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:8.2p1Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
http://www.openwall.com/lists/oss-security/2020/12/02/1

MEDIUM (CVSS: 5.3)

NVT: OPENSSH INFORMATION DISCLOSURE VULNERABILITY (CVE-2016-20012) (OID: 1.3.6.1.4.1.25623.1.0.117777)

22/TCP (SSH)

Summary
OpenBSD OpenSSH is prone to an information disclosure vulnerability.

Vulnerability Detection Result
Installed version: 8.2p1Fixed version: NoneInstallationpath / port: 22/tcp

Solution
No known solution is available as of 16th November, 2021. Information regarding this issue will be updated once solution details are available. Note: This issue is not treated as a security issue by the vendor so no update might be provided in the future.

Vulnerability Insight
OpenSSH 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.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH Information Disclosure Vulnerability (CVE-2016-20012)(OID: 1.3.6.1.4.1.25623.1.0.117777)Version used: 2021-11-16T14:03:35Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:8.2p1Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://github.com/openssh/openssh-portable/pull/270,https://rushter.com/blog/public-ssh-keys/,https://utcc.utoronto.ca/~cks/space/blog/tech/SSHKeysAreInfoLeak

2.18 - 176.16.1.54 (00:17:4G:01:07:BE)

Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	HIGHEST CVSS
176.16.1.54 (00:17:4G:01:07:BE)	2	0	1	1	5.3

Listening Ports

PORT
22/tcp (ssh), 0/NA

Security Issues

M	MEDIUM (CVSS: 5.3) NVT: OPENSSH INFORMATION DISCLOSURE VULNERABILITY (CVE-2016-20012) (OID: 1.3.6.1.4.1.25623.1.0.117777)	22/TCP (SSH)

Summary
OpenBSD OpenSSH is prone to an information disclosure vulnerability.

Vulnerability Detection Result
Installed version: 8.8Fixed version: NoneInstallationpath / port: 22/tcp

Solution
No known solution is available as of 16th November, 2021. Information regarding this issue will be updated once solution details are available. Note: This issue is not treated as a security issue by the vendor so no update might be provided in the future.

Vulnerability Insight
OpenSSH 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.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH Information Disclosure Vulnerability (CVE-2016-20012)(OID: 1.3.6.1.4.1.25623.1.0.117777)Version used: 2021-11-16T14:03:35Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:8.8Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://github.com/openssh/openssh-portable/pull/270,https://rushter.com/blog/public-ssh-keys/,https://utcc.utoronto.ca/~cks/space/blog/tech/SSHKeysAreInfoLeak

L	LOW (CVSS: 2.6) NVT: TCP TIMESTAMPS (OID: 1.3.6.1.4.1.25623.1.0.80091)	0/NA

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
It was detected that the host implements RFC1323/RFC7323.The following timestamps were retrieved with a delay of 1 seconds in-between:Packet 1: 1180590663Packet 2: 1180591792

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.Details:TCP timestamps(OID: 1.3.6.1.4.1.25623.1.0.80091)Version used: 2020-08-24T08:40:10Z

References
http://www.ietf.org/rfc/rfc1323.txt,http://www.ietf.org/rfc/rfc7323.txt,https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152

2.19 - dctrlr01.myco.com (176.16.1.12 / 00:17:4G:01:07:19)

Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	HIGHEST CVSS
dctrlr01.myco.com (176.16.1.12 / 00:17:4G:01:07:19)	1	0	**1**	0	5.0

Listening Ports

PORT
3389/tcp

Security Issues

M

MEDIUM (CVSS: 5)

NVT: SSL/TLS: REPORT WEAK CIPHER SUITES (OID: 1.3.6.1.4.1.25623.1.0.103440)

3389/TCP

Summary
This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

Vulnerability Detection Result
'Weak' cipher suites accepted by this service via the TLSv1.0

protocol:TLS_RSA_WITH_RC4_128_MD5TLS_RSA_WITH_RC4_128_SHA'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:TLS_RSA_WITH_RC4_128_MD5TLS_RSA_WITH_RC4_128_SHA'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:TLS_RSA_WITH_RC4_128_MD5TLS_RSA_WITH_RC4_128_SHA

Solution
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore. Please see the references for more resources supporting you with this task.

Vulnerability Insight
These rules are applied for the evaluation of the cryptographic strength: - RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808) - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000) - 1024 bit RSA authentication is considered to be insecure and therefore as weak - Any cipher considered to be secure for only the next 10 years is considered as medium - Any other cipher is considered as strong

Vulnerability Detection Method
Details:SSL/TLS: Report Weak Cipher Suites(OID: 1.3.6.1.4.1.25623.1.0.103440)Version used: 2021-12-01T13:10:37Z

References
https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1465_update_6.html,https://bettercrypto.org/,https://mozilla.github.io/server-side-tls/ssl-config-generator/

2.20 - dctrlr02.myco.com (176.16.1.13 / 00:17:4G:01:07:1A)

Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	HIGHEST CVSS
dctrlr02.myco.com (176.16.1.13 / 00:17:4G:01:07:1A)	1	0	1	0	5.0

Listening Ports

PORT
3389/tcp

Security Issues

M

MEDIUM (CVSS: 5)

NVT: SSL/TLS: REPORT WEAK CIPHER SUITES (OID: 1.3.6.1.4.1.25623.1.0.103440)

3389/TCP

Summary
This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

Vulnerability Detection Result
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:TLS_RSA_WITH_RC4_128_MD5TLS_RSA_WITH_RC4_128_SHA'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:TLS_RSA_WITH_RC4_128_MD5TLS_RSA_WITH_RC4_128_SHA'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:TLS_RSA_WITH_RC4_128_MD5TLS_RSA_WITH_RC4_128_SHA

Solution
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore. Please see the references for more resources supporting you with this task.

Vulnerability Insight
These rules are applied for the evaluation of the cryptographic strength: - RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808) - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000) - 1024 bit RSA authentication is considered to be insecure and therefore as weak - Any cipher considered to be secure for only the next 10 years is considered as medium - Any other cipher is considered as strong

Vulnerability Detection Method
Details:SSL/TLS: Report Weak Cipher Suites(OID: 1.3.6.1.4.1.25623.1.0.103440)Version used: 2021-12-01T13:10:37Z

References
https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1465_update_6.html,https://bettercrypto.org/,https://mozilla.github.io/server-side-tls/ssl-config-generator/

2.21 - appsvr01.myco.com (176.16.1.14 / 00:17:4G:01:07:18)

Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	HIGHEST CVSS
appsvr01.myco.com (176.16.1.14 / 00:17:4G:01:07:18)	1	0	1	0	5.0

Listening Ports

PORT
3389/tcp

Security Issues

M	MEDIUM (CVSS: 5) NVT: SSL/TLS: REPORT WEAK CIPHER SUITES (OID: 1.3.6.1.4.1.25623.1.0.103440)	3389/TCP

Summary
This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service

the alternative would be to fall back to an even more insecure cleartext communication.

Vulnerability Detection Result
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:TLS_RSA_WITH_RC4_128_MD5TLS_RSA_WITH_RC4_128_SHA'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:TLS_RSA_WITH_RC4_128_MD5TLS_RSA_WITH_RC4_128_SHA'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:TLS_RSA_WITH_RC4_128_MD5TLS_RSA_WITH_RC4_128_SHA

Solution
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore. Please see the references for more resources supporting you with this task.

Vulnerability Insight
These rules are applied for the evaluation of the cryptographic strength: - RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808) - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000) - 1024 bit RSA authentication is considered to be insecure and therefore as weak - Any cipher considered to be secure for only the next 10 years is considered as medium - Any other cipher is considered as strong

Vulnerability Detection Method
Details:SSL/TLS: Report Weak Cipher Suites(OID: 1.3.6.1.4.1.25623.1.0.103440)Version used: 2021-12-01T13:10:37Z

References
https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1465_update_6.html,https://bettercrypto.org/,https://mozilla.github.io/server-side-tls/ssl-config-generator/

2.22 - exchsvr01.myco.com (176.16.1.15 / 00:17:4G:01:07:24)

Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	HIGHEST CVSS
exchsvr01.myco.com (176.16.1.15 / 00:17:4G:01:07:24)	2	0	2	1	5.0

Listening Ports

PORT
3389/tcp, 0/NA

Security Issues

M	MEDIUM (CVSS: 5) NVT: SSL/TLS: REPORT WEAK CIPHER SUITES (OID: 1.3.6.1.4.1.25623.1.0.103440)	3389/TCP

Summary

This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

Vulnerability Detection Result
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:TLS_RSA_WITH_RC4_128_MD5TLS_RSA_WITH_RC4_128_SHA'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:TLS_RSA_WITH_RC4_128_MD5TLS_RSA_WITH_RC4_128_SHA'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:TLS_RSA_WITH_RC4_128_MD5TLS_RSA_WITH_RC4_128_SHA

Solution
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore. Please see the references for more resources supporting you with this task.

Vulnerability Insight
These rules are applied for the evaluation of the cryptographic strength: - RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808) - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000) - 1024 bit RSA authentication is considered to be insecure and therefore as weak - Any cipher considered to be secure for only the next 10 years is considered as medium - Any other cipher is considered as strong

Vulnerability Detection Method
Details:SSL/TLS: Report Weak Cipher Suites(OID: 1.3.6.1.4.1.25623.1.0.103440)Version used: 2021-12-01T13:10:37Z

References
https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1465_update_6.html,https://bettercrypto.org/,https://mozilla.github.io/server-side-tls/ssl-config-generator/

M

MEDIUM (CVSS: 4)

NVT: SSL/TLS: DIFFIE-HELLMAN KEY EXCHANGE INSUFFICIENT DH GROUP STRENGTH VULNERABILITY (OID: 1.3.6.1.4.1.25623.1.0.106223)

3389/TCP

Summary
The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

Vulnerability Detection Result
Server Temporary Key Size: 1024 bits

Impact
An attacker might be able to decrypt the SSL/TLS communication offline.

Solution
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references). For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

Vulnerability Insight
The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

Vulnerability Detection Method
Checks the DHE temporary public key size.Details:SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerab...(OID: 1.3.6.1.4.1.25623.1.0.106223)Version used: 2021-02-12T06:42:15Z

References
https://weakdh.org/,https://weakdh.org/sysadmin.html

L	LOW (CVSS: 2.6) NVT: TCP TIMESTAMPS (OID: 1.3.6.1.4.1.25623.1.0.80091)	0/NA

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
It was detected that the host implements RFC1323/RFC7323.The following timestamps were retrieved with a delay of 1 seconds in-between:Packet 1: 86273391Packet 2: 86273503

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.Details:TCP timestamps(OID: 1.3.6.1.4.1.25623.1.0.80091)Version used: 2020-08-24T08:40:10Z

References
http://www.ietf.org/rfc/rfc1323.txt,http://www.ietf.org/rfc/rfc7323.txt,https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152

2.23 - fsvr01.myco.com (176.16.1.16 / 00:17:4G:01:07:1B)

Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	HIGHEST CVSS
fsvr01.myco.com (176.16.1.16 / 00:17:4G:01:07:1B)	2	0	**1**	1	5.0

Listening Ports

PORT
3389/tcp, 0/NA

Security Issues

M

MEDIUM (CVSS: 5)

NVT: SSL/TLS: REPORT WEAK CIPHER SUITES (OID: 1.3.6.1.4.1.25623.1.0.103440)

3389/TCP

Summary
This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

Vulnerability Detection Result
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:TLS_RSA_WITH_RC4_128_MD5TLS_RSA_WITH_RC4_128_SHA'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:TLS_RSA_WITH_RC4_128_MD5TLS_RSA_WITH_RC4_128_SHA'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:TLS_RSA_WITH_RC4_128_MD5TLS_RSA_WITH_RC4_128_SHA

Solution
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore. Please see the references for more resources supporting you with this task.

Vulnerability Insight
These rules are applied for the evaluation of the cryptographic strength: - RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808) - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000) - 1024 bit RSA authentication is considered to be insecure and therefore as weak - Any cipher considered to be secure for only the next 10 years is considered as medium - Any other cipher is considered as strong

Vulnerability Detection Method
Details:SSL/TLS: Report Weak Cipher Suites(OID: 1.3.6.1.4.1.25623.1.0.103440)Version used: 2021-12-01T13:10:37Z

References
https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1465_update_6.html,https://bettercrypto.org/,https://mozilla.github.io/server-side-tls/ssl-config-generator/

L

LOW (CVSS: 2.6)

NVT: TCP TIMESTAMPS (OID: 1.3.6.1.4.1.25623.1.0.80091)

0/NA

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
It was detected that the host implements RFC1323/RFC7323.The following timestamps were retrieved with a delay of 1 seconds in-between:Packet 1: 1181101164Packet 2: 1181102264

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.Details:TCP timestamps(OID: 1.3.6.1.4.1.25623.1.0.80091)Version used: 2020-08-24T08:40:10Z

References
http://www.ietf.org/rfc/rfc1323.txt,http://www.ietf.org/rfc/rfc7323.txt,https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152

2.24 - sql01.myco.com (176.16.1.17 / 00:17:4G:01:07:1D)

Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	HIGHEST CVSS
sql01.myco.com (176.16.1.17 / 00:17:4G:01:07:1D)	2	0	**2**	1	5.0

Listening Ports

PORT
3389/tcp, 0/NA

Security Issues

M

MEDIUM (CVSS: 5)

NVT: SSL/TLS: REPORT WEAK CIPHER SUITES (OID: 1.3.6.1.4.1.25623.1.0.103440)

3389/TCP

Summary
This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

Vulnerability Detection Result
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:TLS_RSA_WITH_RC4_128_MD5TLS_RSA_WITH_RC4_128_SHA'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:TLS_RSA_WITH_RC4_128_MD5TLS_RSA_WITH_RC4_128_SHA'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:TLS_RSA_WITH_RC4_128_MD5TLS_RSA_WITH_RC4_128_SHA

Solution
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore. Please see the references for more resources supporting you with this task.

Vulnerability Insight
These rules are applied for the evaluation of the cryptographic strength: - RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808) - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as

weak (CVE-2015-4000) - 1024 bit RSA authentication is considered to be insecure and therefore as weak - Any cipher considered to be secure for only the next 10 years is considered as medium - Any other cipher is considered as strong

Vulnerability Detection Method
Details:SSL/TLS: Report Weak Cipher Suites(OID: 1.3.6.1.4.1.25623.1.0.103440)Version used: 2021-12-01T13:10:37Z

References
https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1465_update_6.html,https://bettercrypto.org/,https://mozilla.github.io/server-side-tls/ssl-config-generator/

M MEDIUM (CVSS: 4)

NVT: SSL/TLS: DIFFIE-HELLMAN KEY EXCHANGE INSUFFICIENT DH GROUP STRENGTH VULNERABILITY (OID: 1.3.6.1.4.1.25623.1.0.106223)

3389/TCP

Summary
The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

Vulnerability Detection Result
Server Temporary Key Size: 1024 bits

Impact
An attacker might be able to decrypt the SSL/TLS communication offline.

Solution
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references). For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

Vulnerability Insight
The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

Vulnerability Detection Method
Checks the DHE temporary public key size.Details:SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerab...(OID: 1.3.6.1.4.1.25623.1.0.106223)Version used: 2021-02-12T06:42:15Z

References
https://weakdh.org/,https://weakdh.org/sysadmin.html

L LOW (CVSS: 2.6)

NVT: TCP TIMESTAMPS (OID: 1.3.6.1.4.1.25623.1.0.80091)

0/NA

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
It was detected that the host implements RFC1323/RFC7323.The following timestamps were retrieved with a delay of 1 seconds in-between:Packet 1: 110566668Packet 2: 110566784

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.Details:TCP timestamps(OID: 1.3.6.1.4.1.25623.1.0.80091)Version used: 2020-08-24T08:40:10Z

References
http://www.ietf.org/rfc/rfc1323.txt,http://www.ietf.org/rfc/rfc7323.txt,https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152

2.25 - 176.16.1.71 (F4:8E:38:20:FD:F4)

Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	HIGHEST CVSS
176.16.1.71 (F4:8E:38:20:FD:F4)	2	0	**1**	1	4.8

Listening Ports

PORT
23/tcp (telnet), 0/NA

Security Issues

M

MEDIUM (CVSS: 4.8)

NVT: TELNET UNENCRYPTED CLEARTEXT LOGIN (OID: 1.3.6.1.4.1.25623.1.0.108522)

23/TCP (TELNET)

Summary
The remote host is running a Telnet service that allows cleartext logins over unencrypted connections.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
An attacker can uncover login names and passwords by sniffing traffic to the Telnet service.

Solution
Replace Telnet with a protocol like SSH which supports encrypted connections.

Vulnerability Detection Method
Details:Telnet Unencrypted Cleartext Login(OID: 1.3.6.1.4.1.25623.1.0.108522)Version used: 2020-08-24T08:40:10Z

L	LOW (CVSS: 2.6) NVT: TCP TIMESTAMPS (OID: 1.3.6.1.4.1.25623.1.0.80091)	0/NA

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
It was detected that the host implements RFC1323/RFC7323.The following timestamps were retrieved with a delay of 1 seconds in-between:Packet 1: 118201171Packet 2: 118201281

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.Details:TCP timestamps(OID: 1.3.6.1.4.1.25623.1.0.80091)Version used: 2020-08-24T08:40:10Z

References
http://www.ietf.org/rfc/rfc1323.txt,http://www.ietf.org/rfc/rfc7323.txt,https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152

2.26 - 176.16.1.108 (00:17:4G:01:08:0C)

Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	HIGHEST CVSS
176.16.1.108 (00:17:4G:01:08:0C)	1	0	0	1	2.6

Listening Ports

PORT
0/NA

Security Issues

L

LOW (CVSS: 2.6)

NVT: TCP TIMESTAMPS (OID: 1.3.6.1.4.1.25623.1.0.80091)

0/NA

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
It was detected that the host implements RFC1323/RFC7323.The following timestamps were retrieved with a delay of 1 seconds in-between:Packet 1: 25620286Packet 2: 25621409

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.Details:TCP timestamps(OID: 1.3.6.1.4.1.25623.1.0.80091)Version used: 2020-08-24T08:40:10Z

References
http://www.ietf.org/rfc/rfc1323.txt,http://www.ietf.org/rfc/rfc7323.txt,https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152

2.27 - 176.16.1.185 (00:17:4G:01:08:0E)

Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	HIGHEST CVSS
176.16.1.185 (00:17:4G:01:08:0E)	1	0	0	1	2.6

Listening Ports

PORT
0/NA

Security Issues

L	LOW (CVSS: 2.6) NVT: TCP TIMESTAMPS (OID: 1.3.6.1.4.1.25623.1.0.80091)	0/NA

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
It was detected that the host implements RFC1323/RFC7323.The following timestamps were retrieved with a delay of 1 seconds in-between:Packet 1: 64579195Packet 2: 64579310

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.Details:TCP timestamps(OID: 1.3.6.1.4.1.25623.1.0.80091)Version used: 2020-08-24T08:40:10Z

References
http://www.ietf.org/rfc/rfc1323.txt,http://www.ietf.org/rfc/rfc7323.txt,https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152

2.28 - 176.16.1.186 (00:17:4G:01:08:11)

Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	HIGHEST CVSS
176.16.1.186 (00:17:4G:01:08:11)	1	0	0	1	2.6

Listening Ports

PORT
0/NA

Security Issues

L

LOW (CVSS: 2.6)

NVT: TCP TIMESTAMPS (OID: 1.3.6.1.4.1.25623.1.0.80091)

0/NA

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
It was detected that the host implements RFC1323/RFC7323.The following timestamps were retrieved with a delay of 1 seconds in-between:Packet 1: 64580154Packet 2: 64580266

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.Details:TCP timestamps(OID: 1.3.6.1.4.1.25623.1.0.80091)Version used: 2020-08-24T08:40:10Z

References
http://www.ietf.org/rfc/rfc1323.txt,http://www.ietf.org/rfc/rfc7323.txt,https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152

2.29 - 176.16.1.188 (00:17:4G:01:08:1D)

Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	HIGHEST CVSS
176.16.1.188 (00:17:4G:01:08:1D)	1	0	0	1	2.6

Listening Ports

PORT
0/NA

Security Issues

L LOW (CVSS: 2.6)

NVT: TCP TIMESTAMPS (OID: 1.3.6.1.4.1.25623.1.0.80091)

0/NA

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
It was detected that the host implements RFC1323/RFC7323.The following timestamps were retrieved with a delay of 1 seconds in-between:Packet 1: 64580551Packet 2: 64580663

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.Details:TCP timestamps(OID: 1.3.6.1.4.1.25623.1.0.80091)Version used: 2020-08-24T08:40:10Z

References
http://www.ietf.org/rfc/rfc1323.txt,http://www.ietf.org/rfc/rfc7323.txt,https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152

2.30 - 176.16.1.189 (00:17:4G:01:08:14)

Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	HIGHEST CVSS
176.16.1.189 (00:17:4G:01:08:14)	1	0	0	1	2.6

Listening Ports

PORT
0/NA

Security Issues

L

LOW (CVSS: 2.6)

NVT: TCP TIMESTAMPS (OID: 1.3.6.1.4.1.25623.1.0.80091)

0/NA

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
It was detected that the host implements RFC1323/RFC7323.The following timestamps were retrieved with a delay of 1 seconds in-between:Packet 1: 64574941Packet 2: 64575053

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.Details:TCP timestamps(OID: 1.3.6.1.4.1.25623.1.0.80091)Version used: 2020-08-24T08:40:10Z

References
http://www.ietf.org/rfc/rfc1323.txt,http://www.ietf.org/rfc/rfc7323.txt,https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152

2.31 - 176.16.1.208 (00:17:4G:01:07:A0)

Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	HIGHEST CVSS
176.16.1.208 (00:17:4G:01:07:A0)	1	0	0	1	2.6

Listening Ports

PORT
0/NA

Security Issues

L

LOW (CVSS: 2.6)

NVT: TCP TIMESTAMPS (OID: 1.3.6.1.4.1.25623.1.0.80091)

0/NA

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
It was detected that the host implements RFC1323/RFC7323.The following timestamps were retrieved with a delay of 1 seconds in-between:Packet 1: 64651781Packet 2: 64651896

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.Details:TCP timestamps(OID: 1.3.6.1.4.1.25623.1.0.80091)Version used: 2020-08-24T08:40:10Z

References
http://www.ietf.org/rfc/rfc1323.txt,http://www.ietf.org/rfc/rfc7323.txt,https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152