YourIT!
Your Logo Goes Here

VulScan

Internal Vulnerability Scan Issues Report

Prepared for: Client Company

Prepared by: YourIT Company

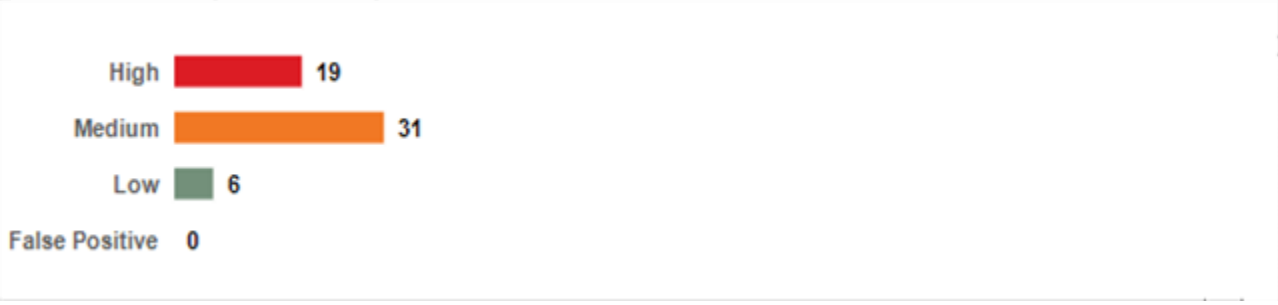
YourIT!
Your Logo Goes Here

Table of Contents

1 - Summary

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

Issues by Severity



Results Filter

Scan Date Range:	02/17/2022 - 03/19/2022
CVSS Filter:	Low (1.0+)
Scan Type:	Internal

Components Scanned

IP Address	Hostname	MAC Address
176.16.1.1	netgwy	00:32:67:GE:F4:5E
176.16.1.12	dctrlr01.myco.com	00:17:4G:02:07:19
176.16.1.13	dctrlr02.myco.com	00:17:4G:02:07:1A
176.16.1.14	appsvr01.myco.com	00:17:4G:02:07:18
176.16.1.15	exchsvr01.myco.com	00:17:4G:02:07:24
176.16.1.16	filesvr01.myco.com	00:17:4G:02:07:1B
176.16.1.17	sqlsvr01.myco.com	00:17:4G:02:07:1D
176.16.1.51	deskpc-klr129u.myco.com	00:17:4G:02:07:CB
176.16.1.52		00:17:4G:02:08:2B

IP Address	Hostname	MAC Address
176.16.1.54		00:17:4G:02:07:BE
176.16.1.57		00:17:4G:02:07:B6
176.16.1.58		00:17:4G:02:07:CC
176.16.1.59		00:17:4G:02:07:C3
176.16.1.61	deskpc-bukapt2.myco.com	00:17:4G:02:07:CD
176.16.1.64		00:17:4G:02:07:C5
176.16.1.65		00:17:4G:02:07:C6
176.16.1.67		00:17:4G:02:07:C8
176.16.1.105	deskpc-amb2rc8.myco.com	00:17:4G:02:07:2F
176.16.1.106	deskpc-e0cvm8b.myco.com	00:17:4G:02:07:30
176.16.1.107	sqlsvr03.myco.com	00:17:4G:02:07:32
176.16.1.108	deskpc-rb3lbp3.myco.com	00:17:4G:02:08:0C
176.16.1.109		C9:45:39:B6:C6:4F
176.16.1.110	deskpc-mvgnq06.myco.com	00:17:4G:02:08:27
176.16.1.111		00:17:4G:02:07:2C
176.16.1.112		00:17:4G:02:08:22
176.16.1.114	deskpc-p1c4fjp.myco.com	00:17:4G:02:08:28
176.16.1.117	deskpc-g0qqu53.myco.com	00:17:4G:02:08:25
176.16.1.118		C9:45:39:B6:C6:4D
176.16.1.122	deskpc-7t6gcbk.myco.com	00:17:4G:02:07:5E
176.16.1.123		00:17:4G:02:07:2D
176.16.1.124	deskpc-n883dvi.myco.com	00:17:4G:02:07:52
176.16.1.125	deskpc-108dsli.myco.com	00:17:4G:02:08:26
176.16.1.129	deskpc-immjr2v.myco.com	00:17:4G:02:08:2A
176.16.1.131	deskpc-5gtvfb3.myco.com	00:17:4G:02:07:60
176.16.1.132		00:17:4G:02:07:61
176.16.1.133	deskpc-elbldbs.myco.com	00:17:4G:02:07:62

IP Address	Hostname	MAC Address
176.16.1.147	hyprvsvr2.myco.com	C9:45:39:B6:C6:4C
176.16.1.148	hyprvsvr1.myco.com	C9:45:39:B6:DC:4E
176.16.1.149	winwkstn10-4.myco.com	00:17:4G:02:07:28
176.16.1.151	deskpc-mgmt01.myco.com	E9:CB:8A:20:53:AC
176.16.1.155	deskpc-c5srli4.myco.com	00:17:4G:02:07:7D
176.16.1.156		00:17:4G:02:07:7B
176.16.1.157	deskpc-534ms45.myco.com	00:17:4G:02:08:23
176.16.1.163		00:17:4G:02:07:85
176.16.1.164	deskpc-adu1dsq.myco.com	00:17:4G:02:07:86
176.16.1.165		00:17:4G:02:07:87
176.16.1.169	deskpc-09upspo.myco.com	00:17:4G:02:08:00
176.16.1.170	deskpc-bdjfflg.myco.com	00:17:4G:02:08:01
176.16.1.171	deskpc-f6ckerq.myco.com	00:17:4G:02:08:02
176.16.1.172	deskpc-lifrcfu.myco.com	00:17:4G:02:08:03
176.16.1.173	deskpc-4171ar0.myco.com	00:17:4G:02:08:04
176.16.1.174	deskpc-f0m1o27.myco.com	00:17:4G:02:08:05
176.16.1.175	deskpc-u1k3naf.myco.com	00:17:4G:02:08:06
176.16.1.176	deskpc-85bjgjt.myco.com	00:17:4G:02:08:07
176.16.1.177	deskpc-4pf2icp.myco.com	00:17:4G:02:08:08
176.16.1.178		00:17:4G:02:07:94
176.16.1.179	deskpc-35egqcc.myco.com	00:17:4G:02:08:0A
176.16.1.180	deskpc-191ijql.myco.com	00:17:4G:02:08:0B
176.16.1.181		00:17:4G:02:08:2C
176.16.1.182		00:17:4G:02:08:0D
176.16.1.193	deskpc-hn95p9q.myco.com	00:17:4G:02:08:1B
176.16.1.204		00:17:4G:02:08:2D
176.16.1.205		00:17:4G:02:08:2E

IP Address	Hostname	MAC Address
176.16.1.206	deskpc-nf6blbc.myco.com	00:17:4G:02:08:2F
176.16.1.210	deskpc-bjen1uq.myco.com	00:17:4G:02:08:30
176.16.1.211	win-tatvq3rem1k.myco.com	00:17:4G:02:07:B3
176.16.1.213	deskpc-07rd86g.myco.com	00:17:4G:02:08:31
176.16.1.219		00:17:4G:02:08:32

2 - Scan Details

2.1 - Jenkins < 2.303.3, < 2.319 Multiple Vulnerabilities - Linux

H	HIGH: (CVSS: 9.8) OID: 1.3.6.1.4.1.25623.1.0.147111	8080/TCP (HTTP-ALT)

Summary
Jenkins is prone to multiple vulnerabilities.

Affected Nodes: Internal
176.16.1.52 (00:17:4G:02:08:2B)

Vulnerability Detection Result
Installed version: 2.290 Fixed version: 2.319 Installation path / port: /

Solution
Update to version 2.319, 2.303.3 LTS or later.

Vulnerability Insight
The following vulnerabilities exist: - CVE-2021-21685, CVE-2021-21686, CVE-2021-21687, CVE-2021-21688, CVE-2021-21689, CVE-2021-21690, CVE-2021-21691, CVE-2021-21692, CVE-2021-21693, CVE-2021-21694, CVE-2021-21695: Bypassing path filtering of agent-to-controller access control - CVE-2021-21696: Agent-to-controller access control allowed writing to sensitive directory used by Pipeline: Shared Groovy Libraries Plugin - CVE-2021-21697: Agent-to-controller access control allows reading/writing most content of build directories

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:Jenkins < 2.303.3, < 2.319 Multiple Vulnerabilities - Linux(OID: 1.3.6.1.4.1.25623.1.0.147111)Version used: 2021-11-10T03:03:45Z

References
https://www.jenkins.io/security/advisory/2021-11-04/

2.2 - nginx 0.6.18 - 1.20.0 1-byte Memory Overwrite Vulnerability

H	HIGH: (CVSS: 9.4) OID: 1.3.6.1.4.1.25623.1.0.117455	80/TCP (HTTP),81/ TCP

Summary
nginx is prone to a 1-byte memory overwrite vulnerability.

Affected Nodes: Internal
176.16.1.58 (00:17:4G:02:07:CC)

Vulnerability Detection Result
Installed version: 1.18.0 Fixed version: 1.20.1/1.21.0 Installation path / port: 80/tcp

Solution
Update to version 1.20.1, 1.21.0 or later.

Vulnerability Insight
A security issue in nginx resolver was identified, which might allow an attacker to cause 1-byte memory overwrite by using a specially crafted DNS response, resulting in worker process crash or, potentially, in arbitrary code execution.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:nginx 0.6.18 - 1.20.0 1-byte Memory Overwrite Vulnerability(OID: 1.3.6.1.4.1.25623.1.0.117455)Version used: 2021-10-18T08:03:29Z

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
http://mailman.nginx.org/pipermail/nginx-announce/2021/000300.html

2.3 - OpenSSH Multiple Vulnerabilities

HIGH: (CVSS: 8.5)
OID: 1.3.6.1.4.1.25623.1.0.806052

22/TCP (SSH)

Summary
OpenSSH is prone to multiple vulnerabilities.

Affected Nodes: Internal
netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

Vulnerability Detection Result
Installed version: 6.6.1p1 Fixed version: 7.0 Installation path / port: 22/tcp

Impact
Successful exploitation will allow an attacker to gain privileges, to conduct impersonation attacks, to conduct brute-force attacks or cause a denial of service.

Solution
Upgrade to OpenSSH 7.0 or later.

Vulnerability Insight
Multiple flaws are due to: - Use-after-free vulnerability in the 'mm_answer_pam_free_ctx' function in monitor.c in sshd. - Vulnerability in 'kbdint_next_device' function in auth2-chall.c in sshd. - Vulnerability in the handler for the MONITOR_REQ_PAM_FREE_CTX request.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH Multiple Vulnerabilities(OID: 1.3.6.1.4.1.25623.1.0.806052)Version used: 2021-10-21T13:57:32Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:6.6.1p1Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
http://seclists.org/fulldisclosure/2015/Aug/54,http://openwall.com/lists/oss-security/2015/07/23/4

2.4 - OpenSSH Privilege Escalation Vulnerability - May16

H	HIGH: (CVSS: 7.8) OID: 1.3.6.1.4.1.25623.1.0.807574	22/TCP (SSH)

Summary
openssh is prone to a privilege escalation vulnerability.

Affected Nodes: Internal
netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

Vulnerability Detection Result
Installed version: 6.6.1p1 Fixed version: 7.2p2-3 Installation path / port: 22/tcp

Impact
Successfully exploiting this issue will allow local users to gain privileges.

Solution
Upgrade to OpenSSH version 7.2p2-3 or later.

Vulnerability Insight
The flaw exists due to an error in 'do_setup_env function' in 'session.c' script in sshd which trigger a crafted environment for the /bin/login program when the UseLogin feature is enabled and PAM is configured to read .pam_environment files in user home directories.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH Privilege Escalation Vulnerability - May16(OID: 1.3.6.1.4.1.25623.1.0.807574)Version used: 2021-10-08T12:01:22Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:6.6.1p1Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://people.canonical.com/~ubuntu-security/cve/2015/CVE-2015-8325.html,https://anongit.mindrot.org/openssh.git/commit/?id=85bdcd7c92fe7ff133bbc4e10a65c91810f88755

2.5 - OpenSSH < 8.1 Integer Overflow Vulnerability

H	HIGH: (CVSS: 7.8) OID: 1.3.6.1.4.1.25623.1.0.108729	22/TCP (SSH)

Summary
OpenSSH is prone to an integer overflow vulnerability.

Affected Nodes: Internal
176.16.1.67 (00:17:4G:02:07:C8)

Vulnerability Detection Result
Installed version: 8.0 Fixed version: 8.1 Installation path / port: 22/tcp

Impact
Successfully exploitation could lead to memory corruption and local code execution.

Solution
Update to version 8.1 or later.

Vulnerability Insight
An exploitable integer overflow bug was found in the private key parsing code for the XMSS key type. This key type is still experimental and support for it is not compiled by default. No user-facing autoconf option exists in portable OpenSSH to enable it.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH < 8.1 Integer Overflow Vulnerability(OID: 1.3.6.1.4.1.25623.1.0.108729)Version used: 2021-07-07T11:00:41Z

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-8.1,https://0day.life/exploits/0day-1009.html,https://cvsweb.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/sshkey-xmss.c.diff?r1=1.5&r2=1.6&f=h

2.6 - OpenSSH Denial of Service And User Enumeration Vulnerabilities (Linux)

H

HIGH: (CVSS: 7.5)

OID: 1.3.6.1.4.1.25623.1.0.809154

22/TCP (SSH)

Summary
openssh is prone to denial of service and user enumeration vulnerabilities.

Affected Nodes: Internal
netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

Vulnerability Detection Result
Installed version: 6.6.1p1 Fixed version: 7.3 Installation path / port: 22/tcp

Impact
Successfully exploiting this issue allows remote attackers to cause a denial of service (crypt CPU consumption) and to enumerate users by leveraging the timing difference between responses when a large password is provided.

Solution
Upgrade to OpenSSH version 7.3 or later.

Vulnerability Insight
Multiple flaws exist due to: - The auth_password function in 'auth-passwd.c' script does not limit password lengths for password authentication. - The sshd in OpenSSH, when SHA256 or SHA512 are used for user password hashing uses BLOWFISH hashing on a static password when the username does not exist and it takes much longer to calculate SHA256/SHA512 hash than BLOWFISH hash.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH Denial of Service And User Enumeration Vulnerabilities (Linux)(OID: 1.3.6.1.4.1.25623.1.0.809154)Version used: 2021-10-12T09:01:32Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:6.6.1p1Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
http://www.openssh.com/txt/release-7.3,http://seclists.org/fulldisclosure/2016/Jul/51,https://security-tracker.debian.org/tracker/CVE-2016-6210,http://openwall.com/lists/oss-security/2016/08/01/2

2.7 - Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSH, D(HE)ater)

H	HIGH: (CVSS: 7.5) 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.

Affected Nodes: Internal
176.16.1.156 (00:17:4G:02:07:7B), 176.16.1.178 (00:17:4G:02:07:94), 176.16.1.219 (00:17:4G:02:08:32), 176.16.1.52 (00:17:4G:02:08:2B), 176.16.1.58 (00:17:4G:02:07:CC), 176.16.1.57 (00:17:4G:02:07:B6), 176.16.1.64 (00:17:4G:02:07:C5), 176.16.1.67 (00:17:4G:02:07:C8), 176.16.1.59 (00:17:4G:02:07:C3), 176.16.1.65 (00:17:4G:02:07:C6), netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

Vulnerability Detection Result
The remote SSH server supports the following DHE KEX algorithm(s): diffie-hellman-group1-sha1 diffie-hellman-group14-sha1 diffie-hellman-group-exchange-sha1 diffie-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

2.8 - Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater)

H	HIGH: (CVSS: 7.5) 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.

Affected Nodes: Internal
deskpc-bdjfflg.myco.com (176.16.1.170 / 00:17:4G:02:08:01), deskpc-rb3lbp3.myco.com (176.16.1.108 / 00:17:4G:02:08:0C), 176.16.1.111 (00:17:4G:02:07:2C), 176.16.1.205 (00:17:4G:02:08:2E), deskpc-85bjgjt.myco.com (176.16.1.176 / 00:17:4G:02:08:07), deskpc-5gtvfb3.myco.com (176.16.1.131 / 00:17:4G:02:07:60), 176.16.1.182 (00:17:4G:02:08:0D), sqlsvr03.myco.com (176.16.1.107 / 00:17:4G:02:07:32), deskpc-adu1dsq.myco.com (176.16.1.164 / 00:17:4G:02:07:86), deskpc-nf6blbc.myco.com (176.16.1.206 / 00:17:4G:02:08:2F), deskpc-bjen1uq.myco.com (176.16.1.210 / 00:17:4G:02:08:30), deskpc-p1c4fjp.myco.com (176.16.1.114 / 00:17:4G:02:08:28), deskpc-7t6gcbk.myco.com (176.16.1.122 / 00:17:4G:02:07:5E), deskpc-mgmt01.myco.com (176.16.1.151 / E9:CB:8A:20:53:AC), 176.16.1.181 (00:17:4G:02:08:2C), 176.16.1.165 (00:17:4G:02:07:87), deskpc-09upspo.myco.com (176.16.1.169 / 00:17:4G:02:08:00), hyprvsvr1.myco.com (176.16.1.148 / C9:45:39:B6:DC:4E), deskpc-e0cvm8b.myco.com (176.16.1.106 / 00:17:4G:02:07:30), deskpc-lifrcfu.myco.com (176.16.1.172 / 00:17:4G:02:08:03), 176.16.1.204 (00:17:4G:02:08:2D), hyprvsvr2.myco.com (176.16.1.147 / C9:45:39:B6:C6:4C), deskpc-191ijql.myco.com (176.16.1.180 / 00:17:4G:02:08:0B), deskpc-f6ckerq.myco.com (176.16.1.171 / 00:17:4G:02:08:02), deskpc-n883dvi.myco.com (176.16.1.124 / 00:17:4G:02:07:52), deskpc-c5srli4.myco.com (176.16.1.155 / 00:17:4G:02:07:7D), deskpc-07rd86g.myco.com (176.16.1.213 / 00:17:4G:02:08:31), win-tatvq3rem1k.myco.com (176.16.1.211 / 00:17:4G:02:07:B3), deskpc-4pf2icp.myco.com (176.16.1.177 / 00:17:4G:02:08:08), deskpc-g0qqu53.myco.com (176.16.1.117 / 00:17:4G:02:08:25), 176.16.1.118 (C9:45:39:B6:C6:4D), 176.16.1.132 (00:17:4G:02:07:61), deskpc-35egqcc.myco.com (176.16.1.179 / 00:17:4G:02:08:0A), deskpc-4171ar0.myco.com (176.16.1.173 / 00:17:4G:02:08:04), winwkstn10-4.myco.com (176.16.1.149 / 00:17:4G:02:07:28), deskpc-108dsli.myco.com (176.16.1.125 / 00:17:4G:02:08:26), deskpc-hn95p9q.myco.com (176.16.1.193 / 00:17:4G:02:08:1B), deskpc-u1k3naf.myco.com (176.16.1.175 / 00:17:4G:02:08:06), 176.16.1.123 (00:17:4G:02:07:2D), deskpc-534ms45.myco.com (176.16.1.157 / 00:17:4G:02:08:23), deskpc-mvgnq06.myco.com (176.16.1.110 / 00:17:4G:02:08:27), deskpc-immjr2v.myco.com (176.16.1.129 / 00:17:4G:02:08:2A), 176.16.1.163 (00:17:4G:02:07:85), deskpc-f0m1o27.myco.com (176.16.1.174 / 00:17:4G:02:08:05), 176.16.1.109 (C9:45:39:B6:C6:4F), deskpc-amb2rc8.myco.com (176.16.1.105 / 00:17:4G:02:07:2F), 176.16.1.112 (00:17:4G:02:08:22), deskpc-elbldbs.myco.com (176.16.1.133 / 00:17:4G:02:07:62)

Vulnerability Detection Result
'DHE' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_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

2.9 - Jenkins < 2.319.3, < 2.334 DoS Vulnerability - Linux

HIGH: (CVSS: 7.5)
OID: 1.3.6.1.4.1.25623.1.0.147621

8080/TCP (HTTP-ALT)

Summary

Jenkins is prone to a denial of service (DoS) vulnerability.

Affected Nodes: Internal
176.16.1.52 (00:17:4G:02:08:2B)

Vulnerability Detection Result
Installed version: 2.290 Fixed version: 2.334 Installation path / port: /

Solution
Update to version 2.334, 2.319.3 LTS or later.

Vulnerability Insight
Jenkins is affected by the XStream library's vulnerability CVE-2021-43859. This library is used by Jenkins to serialize and deserialize various XML files, like global and job config.xml, build.xml, and numerous others. This allows attackers able to submit crafted XML files to Jenkins to be parsed as configuration, e.g. through the POST config.xml API, to cause a denial of service (DoS).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:Jenkins < 2.319.3, < 2.334 DoS Vulnerability - Linux(OID: 1.3.6.1.4.1.25623.1.0.147621)Version used: 2022-02-10T14:05:57Z

References
https://www.jenkins.io/security/advisory/2022-02-09/

2.10 - Jenkins < 2.289.2, < 2.300 Multiple Vulnerabilities - Linux

HIGH: (CVSS: 7.5)
OID: 1.3.6.1.4.1.25623.1.0.146201
8080/TCP (HTTP-ALT)

Summary
Jenkins is prone to multiple vulnerabilities.

Affected Nodes: Internal
176.16.1.52 (00:17:4G:02:08:2B)

Vulnerability Detection Result
Installed version: 2.290 Fixed version: 2.300 Installation path / port: /

Impact
Successful exploitation would allow an attacker to: - cancel queue items and abort builds of jobs for which they have Item/Cancel permission even when they do not have Item/Read permission. - use social engineering techniques to gain administrator access to Jenkins

Solution
Update to version 2.300, 2.289.2 LTS or later.

Vulnerability Insight
The following vulnerabilities exist: - CVE-2021-21670: Improper permission checks allow canceling queue items and aborting builds - CVE-2021-21671: Session fixation

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:Jenkins < 2.289.2, < 2.300 Multiple Vulnerabilities - Linux(OID: 1.3.6.1.4.1.25623.1.0.146201)Version used: 2021-08-17T14:01:00Z

References
https://www.jenkins.io/security/advisory/2021-06-30/

2.11 - nginx <= 1.21.1 Information Disclosure Vulnerability

H	HIGH: (CVSS: 7.5) 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.

Affected Nodes: Internal
176.16.1.58 (00:17:4G:02:07:CC)

Vulnerability Detection Result
Installed version: 1.18.0 Fixed version: None Installation path / 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

2.12 - Deprecated SSH-1 Protocol Detection

H	HIGH: (CVSS: 7.5) OID: 1.3.6.1.4.1.25623.1.0.801993	22/TCP (SSH)

Summary
The host is running SSH and is providing / accepting one or more deprecated versions of the SSH protocol which have known cryptograhic flaws.

Affected Nodes: Internal
netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

Vulnerability Detection Result
The service is providing / accepting the following deprecated versions of the SSH protocol which have known cryptograhic flaws: 1.33 1.5

Impact
Successful exploitation could allows remote attackers to bypass security restrictions and to obtain a client's public host key during a connection attempt and use it to open and authenticate an SSH session to another server with the same access.

Solution
Reconfigure the SSH service to only provide / accept the SSH protocol version SSH-2.

Vulnerability Detection Method
Details:Deprecated SSH-1 Protocol Detection(OID: 1.3.6.1.4.1.25623.1.0.801993)Version used: 2020-08-24T08:40:10Z

References
http://www.kb.cert.org/vuls/id/684820,http://xforce.iss.net/xforce/xfdb/6603

2.13 - SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

HIGH: (CVSS: 7.5)
OID: 1.3.6.1.4.1.25623.1.0.108031

443/TCP (HTTPS)

Summary
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

Affected Nodes: Internal
netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

Vulnerability Detection Result
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32) TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

Solution
The configuration of this services should be changed so that it does not accept the listed 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 vulnerable cipher suites: - 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Vulnerability Detection Method
Details:SSL/TLS: Report Vulnerable Cipher Suites for HTTPS(OID: 1.3.6.1.4.1.25623.1.0.108031)Version used: 2021-09-20T09:01:50Z

References
https://bettercrypto.org/,https://mozilla.github.io/server-side-tls/ssl-config-generator/,https://sweet32.info/

2.14 - OpenSSH schnorr.c Remote Memory Corruption Vulnerability

HIGH: (CVSS: 7.5)
OID: 1.3.6.1.4.1.25623.1.0.105001

22/TCP (SSH)

Summary
OpenSSH is prone to a remote memory-corruption vulnerability.

Affected Nodes: Internal
netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

Vulnerability Detection Result
Installed version: 4.3 Fixed version: See references Installation path / port: 22/tcp

Impact
An attacker can exploit this issue to execute arbitrary code in context of the application. Failed exploits may result in denial-of-service conditions.

Solution
Updates are available. Please see the references for more information.

Vulnerability Insight
The hash_buffer function in schnorr.c in OpenSSH through 6.4, when Makefile.inc is modified to enable the J-PAKE protocol, does not initialize certain data structures, which might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH 'schnorr.c' Remote Memory Corruption Vulnerability(OID: 1.3.6.1.4.1.25623.1.0.105001)Version used: 2019-05-22T07:58:25Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:4.3Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
http://www.securityfocus.com/bid/65230

2.15 - OpenSSH < 4.7 Improper Input Validation Vulnerability

H	HIGH: (CVSS: 7.5) OID: 1.3.6.1.4.1.25623.1.0.150634	22/TCP (SSH)

Summary
ssh in OpenSSH before 4.7 does not properly handle when an untrusted cookie cannot be created and uses a trusted X11 cookie instead, which allows attackers to violate intended policy and gain privileges by causing an X client to be treated as trusted.

Affected Nodes: Internal
netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

Vulnerability Detection Result
Installed version: 4.3 Fixed version: 4.8 Installation path / port: 22/tcp

Solution
Update to version 4.8 or later.

Vulnerability Insight
Please see the references for more information on the vulnerabilities.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH < 4.7 Improper Input Validation Vulnerability(OID: 1.3.6.1.4.1.25623.1.0.150634)Version used: 2021-05-28T11:51:20Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:4.3Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://www.openssh.com/txt/release-4.7

2.16 - OpenSSH <= 5.6 Improper Authentication Vulnerability

H	HIGH: (CVSS: 7.5) OID: 1.3.6.1.4.1.25623.1.0.150632	22/TCP (SSH)

Summary
OpenSSH 5.6 is prone to an authentication bypass vulnerability.

Affected Nodes: Internal
netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

Vulnerability Detection Result
Installed version: 4.3 Fixed version: 5.7 Installation path / port: 22/tcp

Solution
Update to version 5.7 or later.

Vulnerability Insight
Please see the references for more information on the vulnerabilities.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH <= 5.6 Improper Authentication Vulnerability(OID: 1.3.6.1.4.1.25623.1.0.150632)Version used: 2021-05-28T11:51:20Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:4.3Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://github.com/seb-m/jpake

2.17 - OpenSSH Multiple Vulnerabilities Jan17 (Linux)

H	HIGH: (CVSS: 7.3) OID: 1.3.6.1.4.1.25623.1.0.8103256	22/TCP (SSH)

Summary
openssh is prone to multiple vulnerabilities.

Affected Nodes: Internal
netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

Vulnerability Detection Result
Installed version: 6.6.1p1 Fixed version: 7.4 Installation path / port: 22/tcp

Impact
Successfully exploiting this issue allows local users to obtain sensitive private-key information, to gain privileges, conduct a senial-of-service condition and allows remote attackers to execute arbitrary local PKCS#11 modules.

Solution
Upgrade to OpenSSH version 7.4 or later.

Vulnerability Insight
Multiple flaws exist due to: - An 'authfile.c' script does not properly consider the effects of realloc on buffer contents. - The shared memory manager (associated with pre-authentication compression) does not ensure that a bounds check is enforced by all compilers. - The sshd in OpenSSH creates forwarded Unix-domain sockets as root, when privilege separation is not used. - An untrusted search path vulnerability in ssh-agent.c in ssh-agent. - NULL pointer dereference error due to an out-of-sequence NEWKEYS message.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH Multiple Vulnerabilities Jan17 (Linux)(OID: 1.3.6.1.4.1.25623.1.0.8103256)Version used: 2021-10-12T09:28:32Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:6.6.1p1Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://www.openssh.com/txt/release-7.4,http://www.openwall.com/lists/oss-security/2016/12/19/2,http://blog.swiecki.net/2018/01/fuzzing-tcp-servers.html,https://anongit.mindrot.org/openssh.git/commit/?id=28652bca29046f62c7045e933e6b931de1d16737

2.18 - OpenSSH 8.2 < 8.5 Memory Corruption Vulnerability

H | HIGH: (CVSS: 7.1) | 22/TCP (SSH)
OID: 1.3.6.1.4.1.25623.1.0.145538

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

Affected Nodes: Internal
176.16.1.219 (00:17:4G:02:08:32), 176.16.1.52 (00:17:4G:02:08:2B), 176.16.1.58 (00:17:4G:02:07:CC)

Vulnerability Detection Result
Installed version: 8.2p1 Fixed version: 8.5 Installation path / 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

2.19 - OpenSSH 6.2 <= 8.7 Privilege Escalation Vulnerability

H

HIGH: (CVSS: 7)

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.

Affected Nodes: Internal
176.16.1.156 (00:17:4G:02:07:7B), 176.16.1.178 (00:17:4G:02:07:94), 176.16.1.219 (00:17:4G:02:08:32), 176.16.1.52 (00:17:4G:02:08:2B), 176.16.1.58 (00:17:4G:02:07:CC), 176.16.1.57 (00:17:4G:02:07:B6), 176.16.1.64 (00:17:4G:02:07:C5), 176.16.1.67 (00:17:4G:02:07:C8), 176.16.1.59 (00:17:4G:02:07:C3), 176.16.1.65 (00:17:4G:02:07:C6)

Vulnerability Detection Result
Installed version: 6.6.1p1 Fixed version: 8.8 Installation path / 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:6.6.1p1Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

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

2.20 - OpenSSH X Connections Session Hijacking Vulnerability

M

MEDIUM: (CVSS: 6.9)

OID: 1.3.6.1.4.1.25623.1.0.100584

22/TCP (SSH)

Summary
OpenSSH is prone to a vulnerability that allows attackers to hijack forwarded X connections.

Affected Nodes: Internal
netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

Vulnerability Detection Result
Installed version: 4.3 Fixed version: 4.3p2 Installation path / port: 22/tcp

Impact
Successfully exploiting this issue may allow an attacker run arbitrary shell commands with the privileges of the user running the affected application.

Solution

Updates are available. Please see the references for more information.

Vulnerability Detection Method
Details:OpenSSH X Connections Session Hijacking Vulnerability(OID: 1.3.6.1.4.1.25623.1.0.100584)Version used: 2019-05-22T07:58:25Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:4.3Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
http://www.securityfocus.com/bid/28444,http://support.apple.com/kb/HT3137,http://www.openbsd.org/errata41.html,http://www.openbsd.org/errata42.html,http://www.openbsd.org/errata43.html,http://www.openssh.com/txt/release-5.0,http://sourceforge.net/project/shownotes.php?release_id=590180,http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=463011,http://www.securityfocus.com/archive/1/492447,http://aix.software.ibm.com/aix/efixes/security/ssh_advisory.asc,http://support.avaya.com/elmodocs2/security/ASA-2008-205.htm,http://www.globus.org/mail_archive/security-announce/2008/04/msg00000.html,http://support.attachmate.com/techdocs/2374.html#Security_Updates_in_7.0_SP1,http://sunsolve.sun.com/search/document.do?assetkey=1-66-237444-1

2.21 - OpenSSH <= 7.2p1 - Xauth Injection

MEDIUM: (CVSS: 6.4)
OID: 1.3.6.1.4.1.25623.1.0.105581

22/TCP (SSH)

Summary
openssh xauth command injection may lead to forced-command and /bin/false bypass

Affected Nodes: Internal
netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

Vulnerability Detection Result
Installed version: 6.6.1p1 Fixed version: 7.2p2 Installation path / port: 22/tcp

Impact
By injecting xauth commands one gains limited* read/write arbitrary files, information leakage or xauth-connect capabilities.

Solution
Upgrade to OpenSSH version 7.2p2 or later.

Vulnerability Insight
An authenticated user may inject arbitrary xauth commands by sending an x11 channel request that includes a newline character in the x11 cookie. The newline acts as a command separator to the xauth binary. This attack requires the server to have 'X11Forwarding yes' enabled. Disabling it, mitigates this vector.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH <= 7.2p1 - Xauth Injection(OID: 1.3.6.1.4.1.25623.1.0.105581)Version used: 2021-10-14T12:01:33Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:6.6.1p1Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
http://www.openssh.com/txt/release-7.2p2

2.22 - OpenBSD OpenSSH <= 7.9 Multiple Vulnerabilities

MEDIUM: (CVSS: 5.9)
OID: 1.3.6.1.4.1.25623.1.0.117786
22/TCP (SSH)

Summary
OpenBSD OpenSSH is prone to multiple vulnerabilities.

Affected Nodes: Internal
176.16.1.156 (00:17:4G:02:07:7B), 176.16.1.59 (00:17:4G:02:07:C3), netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

Vulnerability Detection Result
Installed version: 6.6.1p1 Fixed version: 8.0 Installation path / 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:6.6.1p1Method: 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

2.23 - OpenBSD OpenSSH Information Disclosure Vulnerability (CVE-2020-14145)

MEDIUM: (CVSS: 5.9)
OID: 1.3.6.1.4.1.25623.1.0.117785
22/TCP (SSH)

Summary
OpenBSD OpenSSH is prone to an information disclosure vulnerability.

Affected Nodes: Internal
176.16.1.156 (00:17:4G:02:07:7B), 176.16.1.219 (00:17:4G:02:08:32), 176.16.1.52 (00:17:4G:02:08:2B), 176.16.1.58 (00:17:4G:02:07:CC), 176.16.1.57 (00:17:4G:02:07:B6), 176.16.1.67 (00:17:4G:02:07:C8), 176.16.1.59 (00:17:4G:02:07:C3)

Vulnerability Detection Result
Installed version: 6.6.1p1 Fixed version: 8.5 Installation path / 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:6.6.1p1Method: 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

2.24 - Jenkins < 2.303.2, < 2.315 HTTP Library Vulnerability - Linux

MEDIUM: (CVSS: 5.8)
OID: 1.3.6.1.4.1.25623.1.0.146872

8080/TCP (HTTP-ALT)

Summary
Jenkins is prone to a vulnerability in the bundled version of commons-httpclient library.

Affected Nodes: Internal
176.16.1.52 (00:17:4G:02:08:2B)

Vulnerability Detection Result
Installed version: 2.290 Fixed version: 2.315 Installation path / port: /

Solution
Update to version 2.315, 2.303.2 LTS or later.

Vulnerability Insight
Jenkins bundles a version of the commons-httpclient library with the vulnerability CVE-2014-3577 that incorrectly verified SSL/TLS certificates, making it susceptible to man-in-the-middle attacks. This library is widely used as a transitive dependency in Jenkins plugins.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:Jenkins < 2.303.2, < 2.315 HTTP Library Vulnerability - Linux(OID: 1.3.6.1.4.1.25623.1.0.146872)Version used: 2021-10-08T08:43:41Z

References
https://www.jenkins.io/security/advisory/2021-10-06/

2.25 - OpenSSH Certificate Validation Security Bypass Vulnerability

MEDIUM: (CVSS: 5.8)
OID: 1.3.6.1.4.1.25623.1.0.105004

22/TCP (SSH)

Summary
OpenSSH is prone to a security-bypass vulnerability.

Affected Nodes: Internal
netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

Vulnerability Detection Result
Installed version: 4.3 Fixed version: See references Installation path / port: 22/tcp

Impact
Attackers can exploit this issue to bypass certain security restrictions and perform unauthorized actions. This may aid in further attacks.

Solution
Updates are available. Please see the references for more information.

Vulnerability Insight
The verify_host_key function in sshconnect.c in the client in OpenSSH 6.6 and earlier allows remote servers to trigger the skipping of SSHFP DNS RR checking by presenting an unacceptable HostCertificate.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH Certificate Validation Security Bypass Vulnerability(OID: 1.3.6.1.4.1.25623.1.0.105004)Version used: 2019-05-22T07:58:25Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:4.3Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
http://www.securityfocus.com/bid/66459

2.26 - OpenSSH sftp-server Security Bypass Vulnerability (Linux)

MEDIUM: (CVSS: 5.3)
OID: 1.3.6.1.4.1.25623.1.0.812051

22/TCP (SSH)

Summary
openssh is prone to a security bypass vulnerability.

Affected Nodes: Internal
176.16.1.156 (00:17:4G:02:07:7B), 176.16.1.59 (00:17:4G:02:07:C3), netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

Vulnerability Detection Result
Installed version: 6.6.1p1 Fixed version: 7.6 Installation path / 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: 2021-10-12T09:28:32Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:6.6.1p1Method: 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

2.27 - Weak Host Key Algorithm(s) (SSH)

M	MEDIUM: (CVSS: 5.3) OID: 1.3.6.1.4.1.25623.1.0.117687	22/TCP (SSH)

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

Affected Nodes: Internal
netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

Vulnerability Detection Result
The remote SSH server supports the following weak host key algorithm(s): host key algorithm | Description ---------- ---------- ssh-dss | Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS)

Solution
Disable the reported weak host key algorithm(s).

Vulnerability Detection Method
Checks the supported host key algorithms of the remote SSH server. Currently weak host key algorithms are defined as the following: - ssh-dss: Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS)Details:Weak Host Key Algorithm(s) (SSH)(OID: 1.3.6.1.4.1.25623.1.0.117687)Version used: 2021-11-24T06:31:19Z

2.28 - Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

M	MEDIUM: (CVSS: 5.3) 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).

Affected Nodes: Internal
176.16.1.156 (00:17:4G:02:07:7B), 176.16.1.67 (00:17:4G:02:07:C8), 176.16.1.59 (00:17:4G:02:07:C3), netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

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 diffie-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

2.29 - OpenSSH Denial of Service Vulnerability - Jan16

MEDIUM: (CVSS: 5.3)
OID: 1.3.6.1.4.1.25623.1.0.806671

22/TCP (SSH)

Summary
openssh is prone to a denial of service (DoS) vulnerability.

Affected Nodes: Internal
netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

Vulnerability Detection Result
Installed version: 6.6.1p1 Fixed version: 7.1p2 Installation path / port: 22/tcp

Impact
Successfully exploiting this issue allow remote attackers to cause a denial of service (out-of-bounds read and application crash).

Solution
Upgrade to OpenSSH version 7.1p2 or later.

Vulnerability Insight
The flaw exists due to an error in 'ssh_packet_read_poll2' function within 'packet.c' script.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH Denial of Service Vulnerability - Jan16(OID: 1.3.6.1.4.1.25623.1.0.806671)Version used: 2021-10-14T12:01:33Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:6.6.1p1Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
http://www.openssh.com/txt/release-7.1p2,https://anongit.mindrot.org/openssh.git/commit/?id=2fecfd486bdba9f51b3a789277bb0733ca36e1c0

2.30 - OpenSSH auth2-gss.c User Enumeration Vulnerability - Linux

MEDIUM: (CVSS: 5.3)
OID: 1.3.6.1.4.1.25623.1.0.813888

22/TCP (SSH)

Summary
OpenSSH is prone to a user enumeration vulnerability.

Affected Nodes: Internal
176.16.1.156 (00:17:4G:02:07:7B), 176.16.1.59 (00:17:4G:02:07:C3)

Vulnerability Detection Result
Installed version: 6.6.1p1 Fixed version: None Installation path / 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:6.6.1p1Method: 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

2.31 - OpenSSH Information Disclosure Vulnerability (CVE-2016-20012)

MEDIUM: (CVSS: 5.3)
OID: 1.3.6.1.4.1.25623.1.0.117777

22/TCP (SSH)

Summary
OpenBSD OpenSSH is prone to an information disclosure vulnerability.

Affected Nodes: Internal
176.16.1.156 (00:17:4G:02:07:7B), 176.16.1.178 (00:17:4G:02:07:94), 176.16.1.219 (00:17:4G:02:08:32), 176.16.1.52 (00:17:4G:02:08:2B), 176.16.1.58 (00:17:4G:02:07:CC), 176.16.1.57 (00:17:4G:02:07:B6), 176.16.1.64 (00:17:4G:02:07:C5), 176.16.1.67 (00:17:4G:02:07:C8), 176.16.1.59 (00:17:4G:02:07:C3), 176.16.1.65 (00:17:4G:02:07:C6), 176.16.1.54 (00:17:4G:02:07:BE), netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

Vulnerability Detection Result
Installed version: 6.6.1p1 Fixed version: None Installation path / 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:6.6.1p1Method: 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

2.32 - OpenSSH < 7.8 User Enumeration Vulnerability - Linux

MEDIUM: (CVSS: 5.3)
OID: 1.3.6.1.4.1.25623.1.0.813864

22/TCP (SSH)

Summary
OpenSSH is prone to a user enumeration vulnerability.

Affected Nodes: Internal
176.16.1.156 (00:17:4G:02:07:7B), 176.16.1.59 (00:17:4G:02:07:C3), netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

Vulnerability Detection Result
Installed version: 6.6.1p1 Fixed version: 7.8 Installation path / 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:6.6.1p1Method: 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

2.33 - Eclipse Jetty Information Disclosure Vulnerability (GHSA-gwcr-j4wh-j3cq)

MEDIUM: (CVSS: 5.3)
OID: 1.3.6.1.4.1.25623.1.0.146099

8080/TCP (HTTP-ALT)

Summary
Eclipse Jetty is prone to an information disclosure vulnerability in the ConcatServlet and WelcomeFilter servlet.

Affected Nodes: Internal
176.16.1.52 (00:17:4G:02:08:2B)

Vulnerability Detection Result
Installed version: 9.4.40.20210413 Fixed version: 9.4.41 Installation path / port: 8080/tcp

Solution
Update to version 9.4.41, 10.0.3, 11.0.3 or later.

Vulnerability Insight
Requests to the ConcatServlet and WelcomeFilter are able to access protected resources within the WEB-INF directory. For example a request to the ConcatServlet with a URI of /concat?/%2557EB-INF/web.xml can retrieve the web.xml file. This can reveal sensitive information regarding the implementation of a web application. This occurs because both ConcatServlet and WelcomeFilter decode the supplied path to verify it is not within the WEB-INF or META-INF directories. It then uses this decoded path to call RequestDispatcher which will also do decoding of the path. This double decoding allows paths with a doubly encoded WEB-INF to bypass this security check.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:Eclipse Jetty Information Disclosure Vulnerability (GHSA-gwcr-j4wh-j3cq)(OID: 1.3.6.1.4.1.25623.1.0.146099)Version used: 2021-08-27T11:01:07Z

Product Detection Result
Product: cpe:/a:eclipse:jetty:9.4.40.20210413Method: MortBay / Eclipse Jetty Detection (HTTP)(OID: 1.3.6.1.4.1.25623.1.0.800953)

References
https://github.com/eclipse/jetty.project/security/advisories/GHSA-gwcr-j4wh-j3cq

2.34 - Eclipse Jetty Information Disclosure Vulnerability (GHSA-vjv5-gp2w-65vm) - Linux

MEDIUM: (CVSS: 5.3)
OID: 1.3.6.1.4.1.25623.1.0.146312

8080/TCP (HTTP-ALT)

Summary
Eclipse Jetty is prone to an information disclosure vulnerability.

Affected Nodes: Internal
176.16.1.52 (00:17:4G:02:08:2B)

Vulnerability Detection Result
Installed version: 9.4.40.20210413 Fixed version: 9.4.43 Installation path / port: 8080/tcp

Impact
The default compliance mode allows requests with URIs that contain a %u002e segment to access protected resources within the WEB-INF directory. For example, a request to /%u002e/WEB-INF/web.xml can retrieve the web.xml file. This can reveal sensitive information regarding the implementation of a web application. Similarly, an encoded null character can prevent correct normalization so that /.%00/WEB-INF/web.xml cal also retrieve the web.xml file.

Solution
Update to version 9.4.43, 10.0.6, 11.0.6 or later. Please see the referenced vendor advisory for a possible workaround.

Vulnerability Insight
URIs can be crafted using some encoded characters to access the content of the WEB-INF directory and/or bypass some security constraints. This is a variation of the vulnerability reported in CVE-2021-28164.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:Eclipse Jetty Information Disclosure Vulnerability (GHSA-vjv5-gp2w-65vm) - L...(OID: 1.3.6.1.4.1.25623.1.0.146312)Version used: 2021-08-27T11:01:07Z

Product Detection Result
Product: cpe:/a:eclipse:jetty:9.4.40.20210413Method: MortBay / Eclipse Jetty Detection (HTTP)(OID: 1.3.6.1.4.1.25623.1.0.800953)

References
https://github.com/eclipse/jetty.project/security/advisories/GHSA-vjv5-gp2w-65vm

2.35 - Weak (Small) Public Key Size(s) (SSH)

MEDIUM: (CVSS: 5.3)
OID: 1.3.6.1.4.1.25623.1.0.150712

22/TCP (SSH)

Summary
The remote SSH server uses a weak (too small) public key size.

Affected Nodes: Internal
netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

Vulnerability Detection Result
The remote SSH server uses a public RSA key with the following weak (too small) size: 1024

Impact
A man-in-the-middle attacker can exploit this vulnerability to record the communication to decrypt the session key and even the messages.

Solution
'- <= 1024 bit for RSA based keys: Install a RSA public key length of 2048 bits or greater, or to switch to more secure key types.

Vulnerability Insight
'- <= 1024 bit for RSA based keys: Best practices require that RSA digital signatures be 2048 or more bits long to provide adequate security. Key lengths of 1024 are considered deprecated since 2011.

Vulnerability Detection Method
Checks the public key size of the remote SSH server. Currently weak (too small) key sizes are defined as the following: - <= 1024 bit for RSA based keysDetails:Weak (Small) Public Key Size(s) (SSH)(OID: 1.3.6.1.4.1.25623.1.0.150712)Version used: 2021-11-24T06:31:19Z

References
https://www.linuxminion.com/ssh-server-public-key-too-small/

2.36 - SSL/TLS: Report Weak Cipher Suites

MEDIUM: (CVSS: 5)
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.

Affected Nodes: Internal
deskpc-rb3lbp3.myco.com (176.16.1.108 / 00:17:4G:02:08:0C), 176.16.1.112 (00:17:4G:02:08:22), filesvr01.myco.com (176.16.1.16 / 00:17:4G:02:07:1B), sqlsvr01.myco.com (176.16.1.17 / 00:17:4G:02:07:1D), exchsvr01.myco.com (176.16.1.15 / 00:17:4G:02:07:24), dctrlr01.myco.com (176.16.1.12 / 00:17:4G:02:07:19), dctrlr02.myco.com (176.16.1.13 / 00:17:4G:02:07:1A), appsvr01.myco.com (176.16.1.14 / 00:17:4G:02:07:18)

Vulnerability Detection Result
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA 'Weak' cipher suites accepted by this service via the TLSv1.1 protocol: TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_RSA_WITH_RC4_128_MD5 TLS_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/

2.37 - Backup File Scanner (HTTP) - Unreliable Detection Reporting

MEDIUM: (CVSS: 5)
OID: 1.3.6.1.4.1.25623.1.0.108975

8080/TCP (HTTP-ALT)

Summary
The script reports backup files left on the web server. Notes: - 'Unreliable Detection' means that a file was detected only based on a HTTP 200 (Found) status code reported by the remote web server when a file was requested. - As the VT 'Backup File Scanner (HTTP)' (OID: 1.3.6.1.4.1.25623.1.0.140853) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

Affected Nodes: Internal
176.16.1.52 (00:17:4G:02:08:2B)

Vulnerability Detection Result
The following backup files were identified (<URL>:<Matching pattern>):
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.GDPR.SpecFlow/Log/log.log/*fingerprint*/.backup:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.GDPR.SpecFlow/Log/log.log/*fingerprint*/.bak:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.G

DPR.SpecFlow/Log/log.log/*fingerprint*/.bkp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.G
DPR.SpecFlow/Log/log.log/*fingerprint*/.copy:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.G
DPR.SpecFlow/Log/log.log/*fingerprint*/.old:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.G
DPR.SpecFlow/Log/log.log/*fingerprint*/.orig:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.G
DPR.SpecFlow/Log/log.log/*fingerprint*/.save:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.G
DPR.SpecFlow/Log/log.log/*fingerprint*/.swp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.G
DPR.SpecFlow/Log/log.log/*fingerprint*/.temp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.G
DPR.SpecFlow/Log/log.log/*fingerprint*/.tmp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.G
DPR.SpecFlow/Log/log.log/*fingerprint*/~:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.G
DPR.SpecFlow/Log/log.log/*view*/.backup:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.G
DPR.SpecFlow/Log/log.log/*view*/.bak:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.G
DPR.SpecFlow/Log/log.log/*view*/.bkp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.G
DPR.SpecFlow/Log/log.log/*view*/.copy:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.G
DPR.SpecFlow/Log/log.log/*view*/.old:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.G
DPR.SpecFlow/Log/log.log/*view*/.orig:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.G
DPR.SpecFlow/Log/log.log/*view*/.save:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.G
DPR.SpecFlow/Log/log.log/*view*/.swp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.G
DPR.SpecFlow/Log/log.log/*view*/.temp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.G
DPR.SpecFlow/Log/log.log/*view*/.tmp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.G
DPR.SpecFlow/Log/log.log/*view*/~:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/allure-
report.zip/*fingerprint*/.backup:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/allure-
report.zip/*fingerprint*/.bak:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/allure-
report.zip/*fingerprint*/.bkp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/allure-
report.zip/*fingerprint*/.copy:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/allure-
report.zip/*fingerprint*/.old:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/allure-
report.zip/*fingerprint*/.orig:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/allure-
report.zip/*fingerprint*/.save:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/allure-
report.zip/*fingerprint*/.swp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/allure-
report.zip/*fingerprint*/.temp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/allure-
report.zip/*fingerprint*/.tmp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/allure-report.zip/*fingerprint*/~:^HTTP/1\.[01]
200 http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/allure-
report.zip/*view*/.backup:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/allure-report.zip/*view*/.bak:^HTTP/1\.[01]
200 http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/allure-
report.zip/*view*/.bkp:^HTTP/1\.[01] 200

http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/allure-report.zip/*view*/.copy:^HTTP/1\.[01] 200 http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/allure-report.zip/*view*/.old:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/allure-report.zip/*view*/.orig:^HTTP/1\.[01] 200 http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/allure-report.zip/*view*/.save:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/allure-report.zip/*view*/.swp:^HTTP/1\.[01] 200 http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/allure-report.zip/*view*/.temp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/allure-report.zip/*view*/.tmp:^HTTP/1\.[01] 200 http://176.16.1.52:8080/job/Debug_CM_for_EU_GDPR/lastSuccessfulBuild/artifact/allure-report.zip/*view*/~:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.HIPAA.SpecFlow/Log/log.log/*fingerprint*/.backup:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.HIPAA.SpecFlow/Log/log.log/*fingerprint*/.bak:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.HIPAA.SpecFlow/Log/log.log/*fingerprint*/.bkp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.HIPAA.SpecFlow/Log/log.log/*fingerprint*/.copy:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.HIPAA.SpecFlow/Log/log.log/*fingerprint*/.old:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.HIPAA.SpecFlow/Log/log.log/*fingerprint*/.orig:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.HIPAA.SpecFlow/Log/log.log/*fingerprint*/.save:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.HIPAA.SpecFlow/Log/log.log/*fingerprint*/.swp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.HIPAA.SpecFlow/Log/log.log/*fingerprint*/.temp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.HIPAA.SpecFlow/Log/log.log/*fingerprint*/.tmp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.HIPAA.SpecFlow/Log/log.log/*fingerprint*/~:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.HIPAA.SpecFlow/Log/log.log/*view*/.backup:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.HIPAA.SpecFlow/Log/log.log/*view*/.bak:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.HIPAA.SpecFlow/Log/log.log/*view*/.bkp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.HIPAA.SpecFlow/Log/log.log/*view*/.copy:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.HIPAA.SpecFlow/Log/log.log/*view*/.old:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.HIPAA.SpecFlow/Log/log.log/*view*/.orig:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.HIPAA.SpecFlow/Log/log.log/*view*/.save:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.HIPAA.SpecFlow/Log/log.log/*view*/.swp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.HIPAA.SpecFlow/Log/log.log/*view*/.temp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.HIPAA.SpecFlow/Log/log.log/*view*/.tmp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.HIPAA.SpecFlow/Log/log.log/*view*/~:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/allure-report.zip/*fingerprint*/.backup:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/allure-report.zip/*fingerprint*/.bak:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/allure-report.zip/*fingerprint*/.bkp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/allure-report.zip/*fingerprint*/.copy:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/allure-

report.zip/*fingerprint*/.old:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/allure-report.zip/*fingerprint*/.orig:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/allure-report.zip/*fingerprint*/.save:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/allure-report.zip/*fingerprint*/.swp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/allure-report.zip/*fingerprint*/.temp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/allure-report.zip/*fingerprint*/.tmp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/allure-report.zip/*fingerprint*/~:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/allure-report.zip/*view*/.backup:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/allure-report.zip/*view*/.bak:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/allure-report.zip/*view*/.bkp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/allure-report.zip/*view*/.copy:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/allure-report.zip/*view*/.old:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/allure-report.zip/*view*/.orig:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/allure-report.zip/*view*/.save:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/allure-report.zip/*view*/.swp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/allure-report.zip/*view*/.temp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/allure-report.zip/*view*/.tmp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_HIPAA_Cloud_env/lastSuccessfulBuild/artifact/allure-report.zip/*view*/~:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_NIST/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.NIST.SpecFlow/Log/log.log/*fingerprint*/.backup:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_NIST/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.NIST.SpecFlow/Log/log.log/*fingerprint*/.bak:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_NIST/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.NIST.SpecFlow/Log/log.log/*fingerprint*/.bkp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_NIST/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.NIST.SpecFlow/Log/log.log/*fingerprint*/.copy:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_NIST/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.NIST.SpecFlow/Log/log.log/*fingerprint*/.old:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_NIST/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.NIST.SpecFlow/Log/log.log/*fingerprint*/.orig:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_NIST/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.NIST.SpecFlow/Log/log.log/*fingerprint*/.save:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_NIST/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.NIST.SpecFlow/Log/log.log/*fingerprint*/.swp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_NIST/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.NIST.SpecFlow/Log/log.log/*fingerprint*/.temp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_NIST/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.NIST.SpecFlow/Log/log.log/*fingerprint*/.tmp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_NIST/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.NIST.SpecFlow/Log/log.log/*fingerprint*/~:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_NIST/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.NIST.SpecFlow/Log/log.log/*view*/.backup:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_NIST/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.NIST.SpecFlow/Log/log.log/*view*/.bak:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_NIST/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.NIST.SpecFlow/Log/log.log/*view*/.bkp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_NIST/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.NIST.SpecFlow/Log/log.log/*view*/.copy:^HTTP/1\.[01] 200

http://176.16.1.52:8080/job/Debug_CM_for_NIST/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.NIST.SpecFlow/Log/log.log/*view*/.old:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_NIST/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.NIST.SpecFlow/Log/log.log/*view*/.orig:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_NIST/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.NIST.SpecFlow/Log/log.log/*view*/.save:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_NIST/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.NIST.SpecFlow/Log/log.log/*view*/.swp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_NIST/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.NIST.SpecFlow/Log/log.log/*view*/.temp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_NIST/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.NIST.SpecFlow/Log/log.log/*view*/.tmp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_CM_for_NIST/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.NIST.SpecFlow/Log/log.log/*view*/~:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_VulScan_E2E/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*fingerprint*/.backup:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_VulScan_E2E/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*fingerprint*/.bak:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_VulScan_E2E/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*fingerprint*/.bkp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_VulScan_E2E/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*fingerprint*/.copy:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_VulScan_E2E/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*fingerprint*/.old:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_VulScan_E2E/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*fingerprint*/.orig:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_VulScan_E2E/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*fingerprint*/.save:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_VulScan_E2E/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*fingerprint*/.swp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_VulScan_E2E/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*fingerprint*/.temp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_VulScan_E2E/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*fingerprint*/.tmp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_VulScan_E2E/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*fingerprint*/~:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_VulScan_E2E/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*view*/.backup:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_VulScan_E2E/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*view*/.bak:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_VulScan_E2E/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*view*/.bkp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_VulScan_E2E/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*view*/.copy:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_VulScan_E2E/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*view*/.old:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_VulScan_E2E/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*view*/.orig:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_VulScan_E2E/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*view*/.save:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_VulScan_E2E/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*view*/.swp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_VulScan_E2E/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*view*/.temp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_VulScan_E2E/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*view*/.tmp:^HTTP/1\.[01] 200
http://176.16.1.52:8080/job/Debug_VulScan_E2E/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*view*/~:^HTTP/1\.[01] 200 http://176.16.1.52:8080/job/VulScan%20autotests%20-%20Beta%20Env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*fingerprint*/.backup:^HTTP/1\.[01] 200 http://176.16.1.52:8080/job/VulScan%20autotests%20-%20Beta%20Env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*fingerprint*/.bak:^HTTP/1\.[01] 200 http://176.16.1.52:8080/job/VulScan%20autotests%20-%20Beta%20Env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*fingerprint*/.bkp:^HTTP/1\.[01] 200 http://176.16.1.52:8080/job/VulScan%20autotests%20-%20Beta%20Env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*fingerp

rint*/.copy:^HTTP/1\.[01] 200 http://176.16.1.52:8080/job/VulScan%20autotests%20-%20Beta%20Env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*fingerprint*/.old:^HTTP/1\.[01] 200 http://176.16.1.52:8080/job/VulScan%20autotests%20-%20Beta%20Env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*fingerprint*/.orig:^HTTP/1\.[01] 200 http://176.16.1.52:8080/job/VulScan%20autotests%20-%20Beta%20Env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*fingerprint*/.save:^HTTP/1\.[01] 200 http://176.16.1.52:8080/job/VulScan%20autotests%20-%20Beta%20Env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*fingerprint*/.swp:^HTTP/1\.[01] 200 http://176.16.1.52:8080/job/VulScan%20autotests%20-%20Beta%20Env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*fingerprint*/.temp:^HTTP/1\.[01] 200 http://176.16.1.52:8080/job/VulScan%20autotests%20-%20Beta%20Env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*fingerprint*/.tmp:^HTTP/1\.[01] 200 http://176.16.1.52:8080/job/VulScan%20autotests%20-%20Beta%20Env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*fingerprint*/~:^HTTP/1\.[01] 200 http://176.16.1.52:8080/job/VulScan%20autotests%20-%20Beta%20Env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*view*/.backup:^HTTP/1\.[01] 200 http://176.16.1.52:8080/job/VulScan%20autotests%20-%20Beta%20Env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*view*/.bak:^HTTP/1\.[01] 200 http://176.16.1.52:8080/job/VulScan%20autotests%20-%20Beta%20Env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*view*/.bkp:^HTTP/1\.[01] 200 http://176.16.1.52:8080/job/VulScan%20autotests%20-%20Beta%20Env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*view*/.copy:^HTTP/1\.[01] 200 http://176.16.1.52:8080/job/VulScan%20autotests%20-%20Beta%20Env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*view*/.old:^HTTP/1\.[01] 200 http://176.16.1.52:8080/job/VulScan%20autotests%20-%20Beta%20Env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*view*/.orig:^HTTP/1\.[01] 200 http://176.16.1.52:8080/job/VulScan%20autotests%20-%20Beta%20Env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*view*/.save:^HTTP/1\.[01] 200 http://176.16.1.52:8080/job/VulScan%20autotests%20-%20Beta%20Env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*view*/.swp:^HTTP/1\.[01] 200 http://176.16.1.52:8080/job/VulScan%20autotests%20-%20Beta%20Env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*view*/.temp:^HTTP/1\.[01] 200 http://176.16.1.52:8080/job/VulScan%20autotests%20-%20Beta%20Env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*view*/.tmp:^HTTP/1\.[01] 200 http://176.16.1.52:8080/job/VulScan%20autotests%20-%20Beta%20Env/lastSuccessfulBuild/artifact/ComplianceManager/ComplianceManager.VulScan.SpecFlow/Log/log.log/*view*/~:^HTTP/1\.[01] 200

Impact
Based on the information provided in this files an attacker might be able to gather sensitive information stored in these files.

Solution
Delete the backup files.

Vulnerability Detection Method
Reports previous enumerated backup files accessible on the remote web server.Details:Backup File Scanner (HTTP) - Unreliable Detection Reporting(OID: 1.3.6.1.4.1.25623.1.0.108975)Version used: 2021-01-21T10:06:42Z

References
http://www.openwall.com/lists/oss-security/2017/10/31/1

2.38 - OpenSSH < 4.7 Improper Authentication Vulnerability

M	MEDIUM: (CVSS: 5) OID: 1.3.6.1.4.1.25623.1.0.150635	22/TCP (SSH)

Summary

OpenSSH, when configured to use S/KEY authentication, is prone to a remoteinformation disclosure weakness. The issue occurs due to the S/KEYchallenge/response system being used for valid accounts. If a remote attackersystematically attempsauthentication against a list of usernames, he can watchthe response to determine which accounts are valid.If 'ChallengeResponseAuthentication' is set to 'Yes', which is the defaultsetting, OpenSSH allows the user to login by using S/KEY in the form of'ssh userid:skey at hostname'.

Affected Nodes: Internal
netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

Vulnerability Detection Result
Installed version: 4.3 Fixed version: 4.7 Installation path / port: 22/tcp

Solution
Update to version 4.7 or later.

Vulnerability Insight
Please see the references for more information on the vulnerabilities.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH < 4.7 Improper Authentication Vulnerability(OID: 1.3.6.1.4.1.25623.1.0.150635)Version used: 2021-05-28T11:51:20Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:4.3Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://cxsecurity.com/issue/WLB-2007040138

2.39 - OpenSSH Denial of Service Vulnerability

MEDIUM: (CVSS: 5)
OID: 1.3.6.1.4.1.25623.1.0.103939

22/TCP (SSH)

Summary
OpenSSH is prone to a remote denial-of-service vulnerability.

Affected Nodes: Internal
netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

Vulnerability Detection Result
Installed version: 4.3 Fixed version: See references Installation path / port: 22/tcp

Impact
Exploiting this issue allows remote attackers to trigger denial-of- service conditions.

Solution
Updates are available. Please see the references for more information.

Vulnerability Insight
The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.

Vulnerability Detection Method
Compare the version retrieved from the banner with the affected range.Details:OpenSSH Denial of Service Vulnerability(OID: 1.3.6.1.4.1.25623.1.0.103939)Version used: 2020-11-25T09:16:10Z

Product Detection Result

Product: cpe:/a:openbsd:openssh:4.3Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
http://www.securityfocus.com/bid/58162

2.40 - SSL/TLS: Certificate Expired

MEDIUM: (CVSS: 5)	443/TCP (HTTPS)
OID: 1.3.6.1.4.1.25623.1.0.103955	

Summary
The remote server's SSL/TLS certificate has already expired.

Affected Nodes: Internal
netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

Vulnerability Detection Result
The certificate of the remote service expired on 2008-05-14 19:36:58. Certificate details: fingerprint (SHA-1) | 99705F26A5FE229588C0EF0CD5CFFE4E4255CF51 fingerprint (SHA-256) | 5E7C8FD7694C8637F1F08B30D8974CE64569796F754704C32F3762CECC673771 issued by | CN=self-signed public key size (bits) | 1024 serial | 01 signature algorithm | sha1WithRSAEncryption subject | CN=0.0.0.0 subject alternative names (SAN) | None valid from | 2007-05-15 19:36:58 UTC valid until | 2008-05-14 19:36:58 UTC

Solution
Replace the SSL/TLS certificate by a new one.

Vulnerability Insight
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

Vulnerability Detection Method
Details:SSL/TLS: Certificate Expired(OID: 1.3.6.1.4.1.25623.1.0.103955)Version used: 2021-11-22T15:32:39Z

2.41 - TCP Sequence Number Approximation Reset Denial of Service Vulnerability

MEDIUM: (CVSS: 5)	0/NA
OID: 1.3.6.1.4.1.25623.1.0.902815	

Summary
TCP services is prone to a denial of service (DoS) vulnerability.

Affected Nodes: Internal
netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

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

Impact
Successful exploitation will allow remote attackers to guess sequence numbers and cause a denial of service to persistent TCP connections by repeatedly injecting a TCP RST packet.

Solution
Please see the referenced advisories for more information on obtaining and applying fixes.

Vulnerability Insight
The flaw is triggered when spoofed TCP Reset packets are received by the targeted TCP stack and will result in loss of availability for the attacked TCP services.

Vulnerability Detection Method
A TCP Reset packet with a different sequence number is sent to the target. A previously open connection is then checked to see if the target closed it or not. Note: At least one open TCP port needs to be available and detected at the target host for this vulnerability check.Details:TCP Sequence Number Approximation Reset Denial of Service Vulnerability(OID: 1.3.6.1.4.1.25623.1.0.902815)Version used: 2022-02-15T13:40:32Z

References
http://xforce.iss.net/xforce/xfdb/15886,https://www.us-cert.gov/ncas/archives/alerts/TA04-111A,http://www-01.ibm.com/support/docview.wss?uid=isg1IY55949,http://www-01.ibm.com/support/docview.wss?uid=isg1IY55950,http://www-01.ibm.com/support/docview.wss?uid=isg1IY62006,https://docs.microsoft.com/en-us/security-updates/securitybulletins/2005/ms05-019,https://docs.microsoft.com/en-us/security-updates/securitybulletins/2006/ms06-064,https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040420-tcp-nonios

2.42 - OpenSSH child_set_env() Function Security Bypass Vulnerability

MEDIUM: (CVSS: 4.9)
OID: 1.3.6.1.4.1.25623.1.0.105003

22/TCP (SSH)

Summary
OpenSSH is prone to a security-bypass vulnerability.

Affected Nodes: Internal
netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

Vulnerability Detection Result
Installed version: 4.3 Fixed version: 6.6 Installation path / port: 22/tcp

Impact
The security bypass allows remote attackers to bypass intended environment restrictions by using a substring located before a wildcard character.

Solution
Updates are available. Please see the references for more information.

Vulnerability Insight
sshd in OpenSSH before 6.6 does not properly support wildcards on AcceptEnv lines in sshd_config.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH 'child_set_env()' Function Security Bypass Vulnerability(OID: 1.3.6.1.4.1.25623.1.0.105003)Version used: 2021-10-15T11:02:56Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:4.3Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
http://www.securityfocus.com/bid/66355

2.43 - Cleartext Transmission of Sensitive Information via HTTP

M	MEDIUM: (CVSS: 4.8) OID: 1.3.6.1.4.1.25623.1.0.108440	8080/TCP (HTTP-ALT)

Summary
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Affected Nodes: Internal
176.16.1.52 (00:17:4G:02:08:2B)

Vulnerability Detection Result
The following input fields where identified (URL:input name): http://176.16.1.52:8080/login:j_password

Impact
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Vulnerability Detection Method
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection. The script is currently checking the following: - HTTP Basic Authentication (Basic Auth) - HTTP Forms (e.g. Login) with input field of type 'password'Details:Cleartext Transmission of Sensitive Information via HTTP(OID: 1.3.6.1.4.1.25623.1.0.108440)Version used: 2020-08-24T15:18:35Z

References
https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management,https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure,https://cwe.mitre.org/data/definitions/319.html

2.44 - Weak Encryption Algorithm(s) Supported (SSH)

M	MEDIUM: (CVSS: 4.3) 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).

Affected Nodes: Internal
176.16.1.67 (00:17:4G:02:07:C8), 176.16.1.59 (00:17:4G:02:07:C3), netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

Vulnerability Detection Result
The remote SSH server supports the following weak client-to-server encryption algorithm(s): 3des-cbc aes128-cbc aes192-cbc aes256-cbc arcfour arcfour128 arcfour256 blowfish-cbc cast128-cbc rijndael-cbc@lysator.liu.se The remote SSH server supports the following weak server-to-client encryption algorithm(s): 3des-cbc aes128-cbc aes192-cbc aes256-cbc arcfour arcfour128 arcfour256 blowfish-cbc cast128-cbc rijndael-cbc@lysator.liu.se

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

2.45 - OpenSSH Security Bypass Vulnerability

MEDIUM: (CVSS: 4.3)
OID: 1.3.6.1.4.1.25623.1.0.806049

22/TCP (SSH)

Summary
OpenSSH is prone to a security bypass vulnerability.

Affected Nodes: Internal
netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

Vulnerability Detection Result
Installed version: 6.6.1p1 Fixed version: 6.9 Installation path / port: 22/tcp

Impact
Successful exploitation will allow remote attackers to bypass intended access restrictions.

Solution
Upgrade to OpenSSH version 6.9 or later.

Vulnerability Insight
The flaw is due to the refusal deadline was not checked within the x11_open_helper function.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH Security Bypass Vulnerability(OID: 1.3.6.1.4.1.25623.1.0.806049)Version used: 2021-10-21T13:57:32Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:6.6.1p1Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
http://openwall.com/lists/oss-security/2015/07/01/10

2.46 - SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

MEDIUM: (CVSS: 4.3)
OID: 1.3.6.1.4.1.25623.1.0.117274

3389/TCP,443/TCP (HTTPS)

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

Affected Nodes: Internal
176.16.1.205 (00:17:4G:02:08:2E), deskpc-nf6blbc.myco.com (176.16.1.206 / 00:17:4G:02:08:2F), deskpc-bjen1uq.myco.com (176.16.1.210 / 00:17:4G:02:08:30), 176.16.1.204 (00:17:4G:02:08:2D), deskpc-07rd86g.myco.com (176.16.1.213 / 00:17:4G:02:08:31), win-tatvq3rem1k.myco.com (176.16.1.211 / 00:17:4G:02:07:B3), deskpc-534ms45.myco.com (176.16.1.157 / 00:17:4G:02:08:23), 176.16.1.112 (00:17:4G:02:08:22), deskpc-klr129u.myco.com (176.16.1.51 / 00:17:4G:02:07:CB), deskpc-bukapt2.myco.com (176.16.1.61 / 00:17:4G:02:07:CD), netgwy (176.16.1.1 / 00:32:67:GE:F4:5E), dctrlr01.myco.com (176.16.1.12 / 00:17:4G:02:07:19)

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

2.47 - Jenkins < 2.319.2, < 2.330 CSRF Vulnerability - Linux

MEDIUM: (CVSS: 4.3)
OID: 1.3.6.1.4.1.25623.1.0.147444

8080/TCP (HTTP-ALT)

Summary
Jenkins is prone to a cross-site request forgery (CSRF) vulnerability.

Affected Nodes: Internal
176.16.1.52 (00:17:4G:02:08:2B)

Vulnerability Detection Result
Installed version: 2.290 Fixed version: 2.330 Installation path / port: /

Impact
This vulnerability allows attackers to trigger build of job without parameters.

Solution
Update to version 2.330, 2.319.2 LTS or later.

Vulnerability Insight
Jenkins does not require POST requests for the HTTP endpoint handling manual build requests when no security realm is set, resulting in a CSRF vulnerability.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:Jenkins < 2.319.2, < 2.330 CSRF Vulnerability - Linux(OID: 1.3.6.1.4.1.25623.1.0.147444)Version used: 2022-01-20T03:03:39Z

References
https://www.jenkins.io/security/advisory/2022-01-12/

2.48 - SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

MEDIUM: (CVSS: 4)
OID: 1.3.6.1.4.1.25623.1.0.105880

3389/TCP

Summary
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

Affected Nodes: Internal
deskpc-rb3lbp3.myco.com (176.16.1.108 / 00:17:4G:02:08:0C)

Vulnerability Detection Result
The following certificates are part of the certificate chain but using insecure signature algorithms: Subject: CN=DESKPC-RB3LBP3.myco.com Signature Algorithm: sha1WithRSAEncryption

Solution
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

Vulnerability Insight
The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use: - Secure Hash Algorithm 1 (SHA-1) - Message Digest 5 (MD5) - Message Digest 4 (MD4) - Message Digest 2 (MD2) Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates. NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive: Fingerprint1 or fingerprint1, Fingerprint2

Vulnerability Detection Method
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.Details:SSL/TLS: Certificate Signed Using A Weak Signature Algorithm(OID: 1.3.6.1.4.1.25623.1.0.105880)Version used: 2021-10-15T11:13:32Z

References
https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

2.49 - SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

MEDIUM: (CVSS: 4)
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).

Affected Nodes: Internal
sqlsvr01.myco.com (176.16.1.17 / 00:17:4G:02:07:1D), exchsvr01.myco.com (176.16.1.15 / 00:17:4G:02:07:24)

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

2.50 - OpenSSH <= 5.8 Multiple DoS Vulnerabilities

MEDIUM: (CVSS: 4)
OID: 1.3.6.1.4.1.25623.1.0.103937

22/TCP (SSH)

Summary
OpenSSH is prone to multiple Denial of Service (DoS) vulnerabilities.

Affected Nodes: Internal
netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

Vulnerability Detection Result
Installed version: 4.3 Fixed version: See references Installation path / port: 22/tcp

Impact
Exploiting this issue allows remote attackers to trigger denial-of-service conditions due to excessive memory consumption.

Solution

Updates are available. Please see the references for details.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH <= 5.8 Multiple DoS Vulnerabilities(OID: 1.3.6.1.4.1.25623.1.0.103937)Version used: 2021-06-07T05:38:52Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:4.3Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
http://www.securityfocus.com/bid/54114,http://seclists.org/fulldisclosure/2011/Aug/2

2.51 - Eclipse Jetty Session Vulnerability (GHSA-m6cp-vxjx-65j6) - Linux

L	LOW: (CVSS: 3.5) OID: 1.3.6.1.4.1.25623.1.0.146164	8080/TCP (HTTP-ALT)

Summary
Eclipse Jetty is prone to a vulnerability in the session management.

Affected Nodes: Internal
176.16.1.52 (00:17:4G:02:08:2B)

Vulnerability Detection Result
Installed version: 9.4.40.20210413 Fixed version: 9.4.41.20210516 Installation path / port: 8080/tcp

Solution
Update to version 9.4.41.v20210516, 10.0.3, 11.0.3 or later.

Vulnerability Insight
If an exception is thrown from the SessionListener#sessionDestroyed() method, then the session ID is not invalidated in the session ID manager. On deployments with clustered sessions and multiple contexts this can result in a session not being invalidated. This can result in an application used on a shared computer being left logged in.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:Eclipse Jetty Session Vulnerability (GHSA-m6cp-vxjx-65j6) - Linux(OID: 1.3.6.1.4.1.25623.1.0.146164)Version used: 2021-08-27T11:01:07Z

Product Detection Result
Product: cpe:/a:eclipse:jetty:9.4.40.20210413Method: MortBay / Eclipse Jetty Detection (HTTP)(OID: 1.3.6.1.4.1.25623.1.0.800953)

References
https://github.com/eclipse/jetty.project/security/advisories/GHSA-m6cp-vxjx-65j6

2.52 - openssh-server Forced Command Handling Information Disclosure Vulnerability

L	LOW: (CVSS: 3.5) OID: 1.3.6.1.4.1.25623.1.0.103503	22/TCP (SSH)

Summary
The auth_parse_options function in auth-options.c in sshd in OpenSSH before 5.7 provides debug messages containing authorized_keys command options, which allows remote authenticated users to obtain potentially sensitive information by reading these messages, as demonstrated by the shared user account required by Gitolite. NOTE: this can cross privilege boundaries because a user account may intentionally have no shell or filesystem access, and therefore may have no nupported way to read an authorized_keys file in its own home directory.

Affected Nodes: Internal
netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

Vulnerability Detection Result
Installed version: 4.3 Fixed version: 5.7 Installation path / port: 22/tcp

Solution
Updates are available. Please see the references for more information.

Vulnerability Detection Method
Details:openssh-server Forced Command Handling Information Disclosure Vulnerability(OID: 1.3.6.1.4.1.25623.1.0.103503)Version used: 2019-05-22T07:58:25Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:4.3Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
http://www.securityfocus.com/bid/51702,http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=657445,https://downloads.avaya.com/css/P8/documents/100161262

2.53 - Weak MAC Algorithm(s) Supported (SSH)

L | LOW: (CVSS: 2.6) | 22/TCP (SSH)
OID: 1.3.6.1.4.1.25623.1.0.105610

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

Affected Nodes: Internal
netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

Vulnerability Detection Result
The remote SSH server supports the following weak client-to-server MAC algorithm(s): hmac-md5 hmac-md5-96 hmac-md5-96-etm@openssh.com hmac-md5-etm@openssh.com hmac-sha1-96 hmac-sha1-96-etm@openssh.com The remote SSH server supports the following weak server-to-client MAC algorithm(s): hmac-md5 hmac-md5-96 hmac-md5-96-etm@openssh.com hmac-md5-etm@openssh.com hmac-sha1-96 hmac-sha1-96-etm@openssh.com

Solution
Disable the reported weak MAC algorithm(s).

Vulnerability Detection Method
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server. Currently weak MAC algorithms are defined as the following: - MD5 based algorithms - 96-bit based algorithms - none algorithmDetails:Weak MAC Algorithm(s) Supported (SSH)(OID: 1.3.6.1.4.1.25623.1.0.105610)Version used: 2021-09-20T11:05:40Z

2.54 - Relative IP Identification number change

L	LOW: (CVSS: 2.6) OID: 1.3.6.1.4.1.25623.1.0.10201	0/NA

Summary
The remote host uses non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host.

Affected Nodes: Internal
deskpc-nf6blbc.myco.com (176.16.1.206 / 00:17:4G:02:08:2F), 176.16.1.181 (00:17:4G:02:08:2C), 176.16.1.165 (00:17:4G:02:07:87), 176.16.1.123 (00:17:4G:02:07:2D), appsvr01.myco.com (176.16.1.14 / 00:17:4G:02:07:18), 176.16.1.205 (00:17:4G:02:08:2E), deskpc-35egqcc.myco.com (176.16.1.179 / 00:17:4G:02:08:0A), 176.16.1.132 (00:17:4G:02:07:61), deskpc-hn95p9q.myco.com (176.16.1.193 / 00:17:4G:02:08:1B), sqlsvr01.myco.com (176.16.1.17 / 00:17:4G:02:07:1D), dctrlr01.myco.com (176.16.1.12 / 00:17:4G:02:07:19), deskpc-85bjgjt.myco.com (176.16.1.176 / 00:17:4G:02:08:07), deskpc-c5srli4.myco.com (176.16.1.155 / 00:17:4G:02:07:7D), 176.16.1.112 (00:17:4G:02:08:22), deskpc-108dsli.myco.com (176.16.1.125 / 00:17:4G:02:08:26)

Vulnerability Detection Result
The target host was found to be vulnerable

Impact
An attacker may use this feature to determine traffic patterns within your network. A few examples (not at all exhaustive) are: 1. A remote attacker can determine if the remote host sent a packet in reply to another request. Specifically, an attacker can use your server as an unwilling participant in a blind portscan of another network. 2. A remote attacker can roughly determine server requests at certain times of the day. For instance, if the server is sending much more traffic after business hours, the server may be a reverse proxy or other remote access device. An attacker can use this information to concentrate his/her efforts on the more critical machines. 3. A remote attacker can roughly estimate the number of requests that a web server processes over a period of time.

Solution
Contact your vendor for a patch

Vulnerability Detection Method
Details:Relative IP Identification number change(OID: 1.3.6.1.4.1.25623.1.0.10201)Version used: 2020-08-24T08:40:10Z

2.55 - OpenSSH CBC Mode Information Disclosure Vulnerability

L	LOW: (CVSS: 2.6) OID: 1.3.6.1.4.1.25623.1.0.100153	22/TCP (SSH)

Summary
OpenSSH is prone to an information disclosure vulnerability.

Affected Nodes: Internal
netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

Vulnerability Detection Result
Installed version: 4.3 Fixed version: 5.2 Installation path / port: 22/tcp

Impact
Successful exploits will allow attackers to obtain four bytes of plaintext from an encrypted session.

Solution
Upgrade to OpenSSH 5.2 or later.

Vulnerability Insight
The flaw is due to the improper handling of errors within an SSH session encrypted with a block cipher algorithm in the Cipher-Block Chaining 'CBC' mode.

Vulnerability Detection Method
Details:OpenSSH CBC Mode Information Disclosure Vulnerability(OID: 1.3.6.1.4.1.25623.1.0.100153)Version used: 2022-02-22T15:13:46Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:4.3Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
http://www.securityfocus.com/bid/32319

2.56 - OpenSSH < 5.1 Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

L	LOW: (CVSS: 1.2)	22/TCP (SSH)
	OID: 1.3.6.1.4.1.25623.1.0.150648	

Summary
OpenBSD OpenSSH is prone to hijack the X11 forwarding port vulnerability.

Affected Nodes: Internal
netgwy (176.16.1.1 / 00:32:67:GE:F4:5E)

Vulnerability Detection Result
Installed version: 4.3 Fixed version: 5.1 Installation path / port: 22/tcp

Solution
Update to version 5.1 or later.

Vulnerability Insight
Please see the references for more information on the vulnerabilities.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH < 5.1 Exposure of Sensitive Information to an Unauthorized Actor Vul...(OID: 1.3.6.1.4.1.25623.1.0.150648)Version used: 2021-11-16T12:48:13Z

Product Detection Result
Product: cpe:/a:openbsd:openssh:4.3Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References
https://www.openssh.com/txt/release-5.1