VulScan

External Vulnerability Scan Issues by Device

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

Prepared for: Client Company

Prepared by: YourIT Company

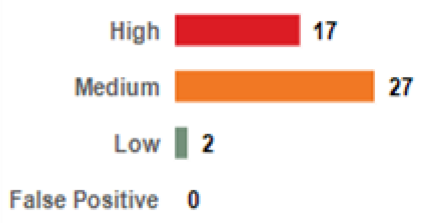
Table of Contents

YourIT!
Your Logo Goes Here

1 - Summary

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

Issues by Severity



Results Filter

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

Components Scanned

IP Address	Hostname	MAC Address
46.35.31.125	myco.com	

2 - Scan Details

2.1 - myco.com (46.35.31.125)

Host Issue Summary

HOST	OPEN PORTS	HIGH	MED	LOW	HIGHEST CVSS
myco.com (46.35.31.125)	3	**17**	**27**	2	9.8

Listening Ports

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

Security Issues

H

HIGH (CVSS: 9.8)

NVT: APACHE HTTP SERVER <= 2.4.52 MULTIPLE VULNERABILITIES - LINUX (OID: 1.3.6.1.4.1.25623.1.0.113837)

80/TCP
(HTTP)

Summary
Apache HTTP Server is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 2.4.7Fixed version: 2.4.53Installationpath / port: 80/tcp

Solution
Update to version 2.4.53 or later.

Vulnerability Insight
The following vulnerabilities exist: - CVE-2022-22719: mod_lua Use of uninitialized value of in r:parsebody - CVE-2022-22720: HTTP request smuggling vulnerability - CVE-2022-22721: Possible buffer overflow with very large or unlimited LimitXMLRequestBody - CVE-2022-23943: mod_sed: Read/write beyond bounds

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:Apache HTTP Server <= 2.4.52 Multiple Vulnerabilities - Linux(OID: 1.3.6.1.4.1.25623.1.0.113837)Version used: 2022-03-21T03:03:41Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.7Method: Apache HTTP Server Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.117232)

References
https://httpd.apache.org/security/vulnerabilities_24.html#2.4.53

HIGH (CVSS: 8.5)

NVT: OPENSSH MULTIPLE VULNERABILITIES (OID: 1.3.6.1.4.1.25623.1.0.806052)

22/TCP (SSH)

Summary
OpenSSH is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 6.6.1p1Fixed version: 7.0Installationpath / 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

HIGH (CVSS: 8.2)

NVT: APACHE HTTP SERVER 2.4.7 - 2.4.51 MULTIPLE VULNERABILITIES - LINUX (OID: 1.3.6.1.4.1.25623.1.0.117854)

80/TCP (HTTP)

Summary
Apache HTTP Server is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 2.4.7Fixed version: 2.4.52Installationpath / port: 80/tcp

Solution
Update to version 2.4.52 or later.

Vulnerability Insight
A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:Apache HTTP Server 2.4.7 - 2.4.51 Multiple Vulnerabilities - Linux(OID: 1.3.6.1.4.1.25623.1.0.117854)Version used: 2021-12-23T12:12:57Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.7Method: Apache HTTP Server Detection Consolidation(OID:

1.3.6.1.4.1.25623.1.0.117232)

References
https://httpd.apache.org/security/vulnerabilities_24.html

H

HIGH (CVSS: 8.1)

NVT: OPENSSH CLIENT INFORMATION LEAK (OID: 1.3.6.1.4.1.25623.1.0.105512)

22/TCP (SSH)

Summary
The OpenSSH client code between 5.4 and 7.1p1 contains experimental support for resuming SSH-connections (roaming). The matching server code has never been shipped, but the client code was enabled by default and could be tricked by a malicious server into leaking client memory to the server, including private client user keys. The authentication of the server host key prevents exploitation by a man-in-the-middle, so this information leak is restricted to connections to malicious or compromised servers.

Vulnerability Detection Result
Installed version: 6.6.1p1Fixed version: 7.1p2Installationpath / port: 22/tcp

Solution
Update to 7.1p2 or newer.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:OpenSSH Client Information Leak(OID: 1.3.6.1.4.1.25623.1.0.105512)Version used: 2021-10-18T09:03:47Z

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

H

HIGH (CVSS: 8.1)

NVT: APACHE HTTP SERVER MAN-IN-THE-MIDDLE ATTACK VULNERABILITY - JULY16 (LINUX) (OID: 1.3.6.1.4.1.25623.1.0.808632)

80/TCP (HTTP)

Summary
Apache HTTP Server is prone to a man-in-the-middle attack vulnerability.

Vulnerability Detection Result
Installed version: 2.4.7Fixed version: 2.4.24Installationpath / port: 80/tcp

Impact
Successful exploitation will allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted proxy header in an HTTP request.

Solution
Update to version 2.4.24, or 2.2.32, or later.

Vulnerability Insight
The flaw is due to 'CGI Servlet' does not protect applications from the presence of untrusted client data in the 'HTTP_PROXY' environment variable.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:Apache HTTP Server Man-in-the-Middle Attack Vulnerability - July16 (Linux)(OID: 1.3.6.1.4.1.25623.1.0.808632)Version used: 2022-04-13T13:17:10Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.7Method: Apache HTTP Server Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.117232)

References
https://www.apache.org/security/asf-httpoxy-response.txt

H

HIGH (CVSS: 7.8)

NVT: OPENSSH PRIVILEGE ESCALATION VULNERABILITY - MAY16 (OID: 1.3.6.1.4.1.25623.1.0.807574)

22/TCP (SSH)

Summary
openssh is prone to a privilege escalation vulnerability.

Vulnerability Detection Result
Installed version: 6.6.1p1Fixed version: 7.2p2-3Installationpath / 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

H

HIGH (CVSS: 7.5)

NVT: APACHE HTTP SERVER OPTIONS MEMORY LEAK VULNERABILITY (OPTIONSBLEED) - VERSION CHECK (OID: 1.3.6.1.4.1.25623.1.0.108252)

80/TCP (HTTP)

Summary
Apache HTTP Server allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed.

Vulnerability Detection Result
Installed version: 2.4.7Fixed version: 2.4.28Installationpath / port: 80/tcp

Impact
The successful exploitation allows the attacker to read chunks of the host's memory.

Solution
Update to Apache HTTP Server 2.4.28. For Apache HTTP Server running version 2.2.34 apply the patch linked in the references. As a workaround the usage of .htaccess should be disabled competely via the 'AllowOverride None' directive within the webservers configuration. Furthermore all <Limit> statements within the webserver configuration needs to be verified for invalid HTTP methods.

Vulnerability Insight
Optionsbleed is a use after free error in the Apache HTTP Server that causes a corrupted Allow header to be constructed in response to HTTP OPTIONS requests. This can leak pieces of arbitrary memory from the server process that may contain secrets. The memory pieces change after multiple requests, so for a vulnerable host an arbitrary number of memory chunks can be leaked. The bug appears if a webmaster tries to use the 'Limit' directive with an invalid HTTP method. Example .htaccess: <Limit abcxyz> </Limit>

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:Apache HTTP Server OPTIONS Memory Leak Vulnerability (Optionsbleed) - Versio...(OID: 1.3.6.1.4.1.25623.1.0.108252)Version used: 2022-04-13T11:57:07Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.7Method: Apache HTTP Server Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.117232)

References
http://openwall.com/lists/oss-security/2017/09/18/2,https://blog.fuzzing-project.org/60-Optionsbleed-HTTP-OPTIONS-method-can-leak-Apaches-server-memory.html,http://www.securityfocus.com/bid/100872,https://archive.apache.org/dist/httpd/patches/apply_to_2.2.34/,https://www.apache.org/dist/httpd/CHANGES_2.4.28

H

HIGH (CVSS: 7.5)

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

22/TCP (SSH)

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

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

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

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

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

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

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

H

HIGH (CVSS: 7.5)

NVT: OPENSSH DENIAL OF SERVICE AND USER ENUMERATION VULNERABILITIES (LINUX) (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.

Vulnerability Detection Result
Installed version: 6.6.1p1Fixed version: 7.3Installationpath / 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: 2022-04-13T13:17:10Z

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

H

HIGH (CVSS: 7.5)

NVT: APACHE HTTP SERVER DENIAL OF SERVICE VULNERABILITY-02 APR18 (LINUX) (OID: 1.3.6.1.4.1.25623.1.0.812849)

80/TCP (HTTP)

Summary
Apache HTTP Server is prone to a denial of service vulnerability.

Vulnerability Detection Result
Installed version: 2.4.7Fixed version: 2.4.30Installationpath / port: 80/tcp

Impact
Successful exploitation will allow an attacker to crash the Apache HTTP Server resulting in denial of service condition.

Solution
Update to version 2.4.30 or later. Please see the references for more information.

Vulnerability Insight
The flaw exists as the Apache HTTP Server fails to sanitize against a specially crafted HTTP request header.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:Apache HTTP Server Denial of Service Vulnerability-02 Apr18 (Linux)(OID: 1.3.6.1.4.1.25623.1.0.812849)Version used: 2022-04-13T07:21:45Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.7Method: Apache HTTP Server Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.117232)

References
https://httpd.apache.org/security/vulnerabilities_24.html

H

HIGH (CVSS: 7.5)

NVT: APACHE HTTP SERVER MOD_AUTH_DIGEST DOS VULNERABILITY (LINUX) (OID: 1.3.6.1.4.1.25623.1.0.812067)

80/TCP (HTTP)

Summary
Apache HTTP Server is prone to a denial-of-service vulnerability.

Vulnerability Detection Result
Installed version: 2.4.7Fixed version: 2.4.25Installationpath / port: 80/tcp

Impact
Successful exploitation will allow remote attackers to cause a denial-of-service condition.

Solution
Update to Apache HTTP Server 2.4.25 or later.

Vulnerability Insight
The flaw exists due to insufficient handling of malicious input to 'mod_auth_digest'.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:Apache HTTP Server 'mod_auth_digest' DoS Vulnerability (Linux)(OID: 1.3.6.1.4.1.25623.1.0.812067)Version used: 2022-04-13T11:57:07Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.7Method: Apache HTTP Server Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.117232)

References
https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2016-2161

H

HIGH (CVSS: 7.5)

NVT: APACHE HTTP SERVER MOD_SESSION_CRYPTO VULNERABILITY (DEC 2016) - LINUX (OID: 1.3.6.1.4.1.25623.1.0.147045)

80/TCP (HTTP)

Summary
Apache HTTP Server is prone to a vulnerability in mod_session_crypto.

Vulnerability Detection Result
Installed version: 2.4.7Fixed version: 2.4.25Installationpath / port: 80/tcp

Solution
Update to version 2.4.25 or later.

Vulnerability Insight
mod_sessioncrypto is encrypting its data/cookie using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default), hence no selectable or builtin authenticated encryption. This makes it vulnerable to padding oracle attacks, particularly with CBC. An authentication tag (SipHash MAC) is now added to prevent such attacks.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:Apache HTTP Server mod_session_crypto Vulnerability (Dec 2016) - Linux(OID: 1.3.6.1.4.1.25623.1.0.147045)Version used: 2021-11-01T14:03:43Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.7Method: Apache HTTP Server Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.117232)

References
https://httpd.apache.org/security/vulnerabilities_24.html

H

HIGH (CVSS: 7.5)

NVT: APACHE HTTP SERVER < 2.4.39 MOD_AUTH_DIGEST ACCESS CONTROL BYPASS VULNERABILITY (LINUX) (OID: 1.3.6.1.4.1.25623.1.0.142220)

80/TCP (HTTP)

Summary
In Apache HTTP Server, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.

Vulnerability Detection Result
Installed version: 2.4.7Fixed version: 2.4.39Installationpath / port: 80/tcp

Solution
Update to version 2.4.39 or later.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:Apache HTTP Server < 2.4.39 mod_auth_digest Access Control Bypass Vulnerabil...(OID: 1.3.6.1.4.1.25623.1.0.142220)Version used: 2021-09-02T13:01:30Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.7Method: Apache HTTP Server Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.117232)

References
https://httpd.apache.org/security/vulnerabilities_24.html

H

HIGH (CVSS: 7.5)

NVT: APACHE HTTP SERVER < 2.4.38 MOD_SESSION_COOKIE VULNERABILITY (LINUX) (OID: 1.3.6.1.4.1.25623.1.0.141964)

80/TCP (HTTP)

Summary
In Apache HTTP Server mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

Vulnerability Detection Result
Installed version: 2.4.7Fixed version: 2.4.38Installationpath / port: 80/tcp

Solution
Update to version 2.4.38 or later.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:Apache HTTP Server < 2.4.38 mod_session_cookie Vulnerability (Linux)(OID: 1.3.6.1.4.1.25623.1.0.141964)Version used: 2021-09-02T13:01:30Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.7Method: Apache HTTP Server Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.117232)

References
https://httpd.apache.org/security/vulnerabilities_24.html

H

HIGH (CVSS: 7.5)

NVT: APACHE HTTP SERVER < 2.4.48 NULL POINTER DEREFERENCE VULNERABILITY - LINUX (OID: 1.3.6.1.4.1.25623.1.0.112905)

80/TCP (HTTP)

Summary
Apache HTTP Server is prone to a NULL pointer dereference vulnerability.

Vulnerability Detection Result
Installed version: 2.4.7Fixed version: 2.4.48Installationpath / port: 80/tcp

Impact
Successful exploitation will allow an attacker to crash the server.

Solution
Update to version 2.4.48 or later.

Vulnerability Insight
Apache HTTP Server protocol handler for the HTTP/2 protocol checks received request headers against the size limitations as configured for the server and used for the HTTP/1 protocol as well. On violation of these restrictions an HTTP response is sent to the client with a status code indicating why the request was rejected. This rejection response was not fully initialised in the HTTP/2 protocol handler if the offending header was the very first one received or appeared in a footer. This led to a NULL pointer dereference on initialised memory, crashing reliably the child process.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:Apache HTTP Server < 2.4.48 NULL Pointer Dereference Vulnerability - Linux(OID: 1.3.6.1.4.1.25623.1.0.112905)Version used: 2021-08-24T06:00:58Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.7Method: Apache HTTP Server Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.117232)

References
https://httpd.apache.org/security/vulnerabilities_24.html

H

HIGH (CVSS: 7.3)

NVT: OPENSSH MULTIPLE VULNERABILITIES JAN17 (LINUX) (OID: 1.3.6.1.4.1.25623.1.0.8103256)

22/TCP (SSH)

Summary
openssh is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 6.6.1p1Fixed version: 7.4Installationpath / 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: 2022-04-13T11:57:07Z

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

HIGH (CVSS: 7)

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

22/TCP (SSH)

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

Vulnerability Detection Result
Installed version: 6.6.1p1Fixed version: 8.8Installationpath / port: 22/tcp

Solution
Update to version 8.8 or later.

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

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

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

M

MEDIUM (CVSS: 6.8)

NVT: APACHE HTTP SERVER MULTIPLE VULNERABILITIES MAY15 (OID: 1.3.6.1.4.1.25623.1.0.805638)

80/TCP (HTTP)

Summary
Apache HTTP Server is prone to a denial of service vulnerability.

Vulnerability Detection Result
Installed version: 2.4.7Fixed version: 2.4.10Installationpath / port: 80/tcp

Impact
Successful exploitation will allow a remote attacker to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives.

Solution
Update to version 2.4.10 or later.

Vulnerability Insight
Multiple flaws are due to: - Vulnerability in the WinNT MPM component within the 'winnt_accept' function in server/mpm/winnt/child.c script that is triggered when the default AcceptFilter is used. - Vulnerability in the mod_deflate module that is triggered when handling highly compressed bodies. - A race condition in the mod_status module that is triggered as user-supplied input is not properly validated when handling the scoreboard. - Vulnerability in the mod_cgid module that is triggered when used to host CGI scripts that do not consume standard input.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:Apache HTTP Server Multiple Vulnerabilities May15(OID: 1.3.6.1.4.1.25623.1.0.805638)Version used: 2022-04-14T06:42:08Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.7Method: Apache HTTP Server Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.117232)

References
http://httpd.apache.org/security/vulnerabilities_24.html,http://www.rapid7.com/db/vulnerabilities/apache-httpd-cve-2014-8109

M

MEDIUM (CVSS: 6.8)

NVT: APACHE HTTP SERVER MULTIPLE VULNERABILITIES (SEP 2014) - LINUX (OID: 1.3.6.1.4.1.25623.1.0.147048)

80/TCP (HTTP)

Summary
Apache HTTP Server is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 2.4.7Fixed version: 2.4.12Installationpath / port: 80/tcp

Solution
Update to version 2.2.29, 2.4.12 or later.

Vulnerability Insight
The following vulnerabilities exist: - CVE-2013-5704: HTTP trailers could be used to replace HTTP headers late during request processing, potentially undoing or otherwise confusing modules that examined or modified request headers earlier. This fix adds the 'MergeTrailers' directive to restore legacy behavior. - CVE-2014-0118: A resource consumption flaw was found in

mod_deflate. If request body decompression was configured (using the 'DEFLATE' input filter), a remote attacker could cause the server to consume significant memory and/or CPU resources. The use of request body decompression is not a common configuration. - CVE-2014-0226: A race condition was found in mod_status. An attacker able to access a public server status page on a server using a threaded MPM could send a carefully crafted request which could lead to a heap buffer overflow. Note that it is not a default or recommended configuration to have a public accessible server status page. - CVE-2014-0231: A flaw was found in mod_cgid. If a server using mod_cgid hosted CGI scripts which did not consume standard input, a remote attacker could cause child processes to hang indefinitely, leading to denial of service.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:Apache HTTP Server Multiple Vulnerabilities (Sep 2014) - Linux(OID: 1.3.6.1.4.1.25623.1.0.147048)Version used: 2021-11-01T03:59:12Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.7Method: Apache HTTP Server Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.117232)

References
https://httpd.apache.org/security/vulnerabilities_22.html,https://httpd.apache.org/security/vulnerabilities_24.html

M

MEDIUM (CVSS: 6.4)

NVT: OPENSSH <= 7.2P1 - XAUTH INJECTION (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

Vulnerability Detection Result
Installed version: 6.6.1p1Fixed version: 7.2p2Installationpath / 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

M

MEDIUM (CVSS: 6.1)

NVT: APACHE HTTP SERVER 2.4.0 - 2.4.40 MULTIPLE VULNERABILITIES (LINUX) (OID: 1.3.6.1.4.1.25623.1.0.114143)

80/TCP (HTTP)

Summary

Apache HTTP Server is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 2.4.7Fixed version: 2.4.41Installationpath / port: 80/tcp

Solution
Update to version 2.4.41 or later.

Vulnerability Insight
Apache HTTP server is prone to multiple vulnerabilities: - A limited cross-site scripting issue affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed. (CVE-2019-10092) - Redirects configured with mod_rewrite that were intended to be self referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL. (CVE-2019-10098)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:Apache HTTP Server 2.4.0 - 2.4.40 Multiple Vulnerabilities (Linux)(OID: 1.3.6.1.4.1.25623.1.0.114143)Version used: 2021-09-02T13:01:30Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.7Method: Apache HTTP Server Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.117232)

References
https://httpd.apache.org/security/vulnerabilities_24.html

M	MEDIUM (CVSS: 6.1) NVT: APACHE HTTP SERVER CRLF INJECTION VULNERABILITY (DEC 2016) - LINUX (OID: 1.3.6.1.4.1.25623.1.0.147044)	80/TCP (HTTP)

Summary
Apache HTTP Server is prone to a CRLF injection vulnerability.

Vulnerability Detection Result
Installed version: 2.4.7Fixed version: 2.4.25Installationpath / port: 80/tcp

Solution
Update to version 2.2.32, 2.4.25 or later.

Vulnerability Insight
Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated to prohibit CR or LF injection into the 'Location' or other outbound header key or value.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:Apache HTTP Server CRLF Injection Vulnerability (Dec 2016) - Linux(OID: 1.3.6.1.4.1.25623.1.0.147044)Version used: 2021-11-01T14:03:43Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.7Method: Apache HTTP Server Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.117232)

References
https://httpd.apache.org/security/vulnerabilities_22.html,https://httpd.apache.org/security/vulnerabilities_24.html

M

MEDIUM (CVSS: 6.1)

NVT: APACHE HTTP SERVER 2.4.0 < 2.4.42 MULTIPLE VULNERABILITIES (LINUX) (OID: 1.3.6.1.4.1.25623.1.0.143671)

80/TCP (HTTP)

Summary
Apache HTTP Server is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 2.4.7Fixed version: 2.4.42Installationpath / port: 80/tcp

Solution
Update to version 2.4.42 or later.

Vulnerability Insight
Apache HTTP Server is prone to multiple vulnerabilities: - mod_rewrite CWE-601 open redirect (CVE-2020-1927) - mod_proxy_ftp use of uninitialized value (CVE-2020-1934)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:Apache HTTP Server 2.4.0 < 2.4.42 Multiple Vulnerabilities (Linux)(OID: 1.3.6.1.4.1.25623.1.0.143671)Version used: 2021-07-22T02:00:50Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.7Method: Apache HTTP Server Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.117232)

References
https://httpd.apache.org/security/vulnerabilities_24.html

M

MEDIUM (CVSS: 5.9)

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

22/TCP (SSH)

Summary
OpenBSD OpenSSH is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 6.6.1p1Fixed version: 8.0Installationpath / port: 22/tcp

Solution
Update to version 8.0 or later.

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

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

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

MEDIUM (CVSS: 5.9)

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

22/TCP (SSH)

Summary
OpenBSD OpenSSH is prone to an information disclosure vulnerability.

Vulnerability Detection Result
Installed version: 6.6.1p1Fixed version: 8.5Installationpath / port: 22/tcp

Solution
Update to version 8.5 or later.

Vulnerability Insight
The client side in OpenSSH has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client).

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

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

MEDIUM (CVSS: 5.3)

NVT: WEAK HOST KEY ALGORITHM(S) (SSH) (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).

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

MEDIUM (CVSS: 5.3)

NVT: APACHE HTTP SERVER 2.4.1 < 2.4.24 IP SPOOFING VULNERABILITY (LINUX) (OID: 1.3.6.1.4.1.25623.1.0.144376)

80/TCP (HTTP)

Summary
Apache HTTP Server is prone to an IP address spoofing vulnerability when proxying using mod_remoteip and mod_rewrite.

Vulnerability Detection Result
Installed version: 2.4.7Fixed version: 2.4.24Installationpath / port: 80/tcp

Solution
Update to version 2.4.24 or later.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:Apache HTTP Server 2.4.1 < 2.4.24 IP Spoofing Vulnerability (Linux)(OID: 1.3.6.1.4.1.25623.1.0.144376)Version used: 2021-07-22T02:00:50Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.7Method: Apache HTTP Server Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.117232)

References
https://httpd.apache.org/security/vulnerabilities_24.html

M

MEDIUM (CVSS: 5.3)

NVT: APACHE HTTP SERVER < 2.4.39 URL NORMALIZATION VULNERABILITY (LINUX) (OID: 1.3.6.1.4.1.25623.1.0.142228)

80/TCP (HTTP)

Summary
When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.

Vulnerability Detection Result
Installed version: 2.4.7Fixed version: 2.4.39Installationpath / port: 80/tcp

Solution
Update to version 2.4.39 or later.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:Apache HTTP Server < 2.4.39 URL Normalization Vulnerability (Linux)(OID: 1.3.6.1.4.1.25623.1.0.142228)Version used: 2021-09-02T13:01:30Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.7Method: Apache HTTP Server Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.117232)

References
https://httpd.apache.org/security/vulnerabilities_24.html

M

MEDIUM (CVSS: 5.3)

NVT: APACHE HTTP SERVER 2.4.6 - 2.4.46 TUNNELING MISCONFIGURATION VULNERABILITY - LINUX (OID: 1.3.6.1.4.1.25623.1.0.112898)

80/TCP (HTTP)

Summary
Apache HTTP Server is prone to a tunneling misconfiguration vulnerability.

Vulnerability Detection Result
Installed version: 2.4.7Fixed version:	2.4.48Installationpath / port:	80/tcp

Solution
Update to version 2.4.48 or later.

Vulnerability Insight
mod_proxy_wstunnel configured on an URL that is not necessarily upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:Apache HTTP Server 2.4.6 - 2.4.46 Tunneling Misconfiguration Vulnerability -...(OID: 1.3.6.1.4.1.25623.1.0.112898)Version used: 2021-08-24T09:01:06Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.7Method: Apache HTTP Server Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.117232)

References
https://httpd.apache.org/security/vulnerabilities_24.html

M

MEDIUM (CVSS: 5.3)

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

22/TCP (SSH)

Summary
OpenBSD OpenSSH is prone to an information disclosure vulnerability.

Vulnerability Detection Result
Installed version: 6.6.1p1Fixed version:	NoneInstallationpath / port:	22/tcp

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

Vulnerability Insight
OpenSSH allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session.

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

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

M

MEDIUM (CVSS: 5.3)

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

22/TCP (SSH)

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

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

Impact
An attacker can quickly break individual connections.

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

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

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

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

M

MEDIUM (CVSS: 5.3)

NVT: OPENSSH DENIAL OF SERVICE VULNERABILITY - JAN16 (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.

Vulnerability Detection Result
Installed version: 6.6.1p1Fixed version: 7.1p2Installationpath / 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

MEDIUM (CVSS: 5.3)

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

22/TCP (SSH)

Summary
OpenSSH is prone to a user enumeration vulnerability.

Vulnerability Detection Result
Installed version: 6.6.1p1Fixed version: 7.8Installationpath / port: 22/tcp

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

Solution
Update to version 7.8 or later.

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

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

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

MEDIUM (CVSS: 5.3)

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

22/TCP (SSH)

Summary
OpenSSH is prone to a user enumeration vulnerability.

Vulnerability Detection Result
Installed version: 6.6.1p1Fixed version: NoneInstallationpath / port: 22/tcp

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

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

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

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

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

M

MEDIUM (CVSS: 5.3)

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

22/TCP (SSH)

Summary
openssh is prone to a security bypass vulnerability.

Vulnerability Detection Result
Installed version: 6.6.1p1Fixed version: 7.6Installationpath / port: 22/tcp

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

Solution
Upgrade to OpenSSH version 7.6 or later.

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

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

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

M

MEDIUM (CVSS: 5)

NVT: APACHE HTTP SERVER MOD_LUA DENIAL OF SERVICE VULNERABILITY -01 MAY15 (OID: 1.3.6.1.4.1.25623.1.0.805616)

80/TCP (HTTP)

Summary
Apache HTTP Server is prone to a denial of service vulnerability.

Vulnerability Detection Result
Installed version: 2.4.7Fixed version: 2.4.13Installationpath / port: 80/tcp

Impact
Successful exploitation will allow a remote attacker to cause a denial of service via some crafted dimension.

Solution

Update to version 2.4.13 or later.

Vulnerability Insight
Flaw is due to vulnerability in lua_websocket_read function in lua_request.c in the mod_lua module.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:Apache HTTP Server 'mod_lua' Denial of Service Vulnerability -01 May15(OID: 1.3.6.1.4.1.25623.1.0.805616)Version used: 2022-04-14T06:42:08Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.7Method: Apache HTTP Server Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.117232)

References
https://bugs.mageia.org/show_bug.cgi?id=15428,http://svn.apache.org/repos/asf/httpd/httpd/branches/2.4.x/CHANGES

M

MEDIUM (CVSS: 5)

NVT: APACHE HTTP SERVER DOS VULNERABILITY (SEP 2014) - LINUX (OID: 1.3.6.1.4.1.25623.1.0.147046)

80/TCP (HTTP)

Summary
Apache HTTP Server is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result
Installed version: 2.4.7Fixed version: 2.4.12Installationpath / port: 80/tcp

Solution
Update to version 2.4.12 or later.

Vulnerability Insight
A NULL pointer deference was found in mod_cache. A malicious HTTP server could cause a crash in a caching forward proxy configuration. This crash would only be a denial of service if using a threaded MPM.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:Apache HTTP Server DoS Vulnerability (Sep 2014) - Linux(OID: 1.3.6.1.4.1.25623.1.0.147046)Version used: 2021-11-01T03:59:12Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.7Method: Apache HTTP Server Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.117232)

References
https://httpd.apache.org/security/vulnerabilities_24.html

M

MEDIUM (CVSS: 5)

NVT: APACHE HTTP SERVER MULTIPLE VULNERABILITIES AUGUST15 (LINUX) (OID: 1.3.6.1.4.1.25623.1.0.806018)

80/TCP (HTTP)

Summary
Apache HTTP Server is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 2.4.7Fixed version: 2.4.14Installationpath / port: 80/tcp

Impact

Successful exploitation will allow remote attackers to bypass intended access restrictions in opportunistic circumstances and to cause cache poisoning or credential hijacking if an intermediary proxy is in use.

Solution
Update to version 2.4.14 or later.

Vulnerability Insight
Multiple flaws are due to: - an error in 'ap_some_auth_required' function in 'server/request.c' script which does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting. - an error in chunked transfer coding implementation.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:Apache HTTP Server Multiple Vulnerabilities August15 (Linux)(OID: 1.3.6.1.4.1.25623.1.0.806018)Version used: 2022-04-14T06:42:08Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.7Method: Apache HTTP Server Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.117232)

References
http://www.apache.org/dist/httpd/CHANGES_2.4,http://httpd.apache.org/security/vulnerabilities_24.html

M

MEDIUM (CVSS: 5)

NVT: ENABLED DIRECTORY LISTING DETECTION (OID: 1.3.6.1.4.1.25623.1.0.111074)

80/TCP (HTTP)

Summary
The script attempts to identify directories with an enabled directory listing.

Vulnerability Detection Result
The following directories with an enabled directory listing were identified:http://myco.com/sharedhttp://myco.com/shared/errorhttp://myco.com/shared/error/includeshttp://myco.com/shared/templatesPlease review the content manually.

Impact
Based on the information shown an attacker might be able to gather additional info about the structure of this application.

Solution
If not needed disable the directory listing within the webservers config.

Vulnerability Detection Method
Check the detected directories if a directory listing is enabled.Details:Enabled Directory Listing Detection(OID: 1.3.6.1.4.1.25623.1.0.111074)Version used: 2020-08-24T15:18:35Z

References
https://www.owasp.org/index.php/OWASP_Periodic_Table_of_Vulnerabilities_-_Directory_Indexing

M

MEDIUM (CVSS: 5)

NVT: APACHE HTTP SERVER MULTIPLE VULNERABILITIES (MAR 2014) - LINUX (OID: 1.3.6.1.4.1.25623.1.0.147047)

80/TCP (HTTP)

Summary
Apache HTTP Server is prone to multiple vulnerabilities.

Vulnerability Detection Result

Installed version: 2.4.7Fixed version: 2.4.9Installationpath / port: 80/tcp

Solution
Update to version 2.2.27, 2.4.9 or later.

Vulnerability Insight
The following vulnerabilities exist: - CVE-2013-6438: XML parsing code in mod_dav incorrectly calculates the end of the string when removing leading spaces and places a NUL character outside the buffer, causing random crashes. This XML parsing code is only used with DAV provider modules that support DeltaV, of which the only publicly released provider is mod_dav_svn. - CVE-2014-0098: A flaw was found in mod_log_config. A remote attacker could send a specific truncated cookie causing a crash. This crash would only be a denial of service if using a threaded MPM.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:Apache HTTP Server Multiple Vulnerabilities (Mar 2014) - Linux(OID: 1.3.6.1.4.1.25623.1.0.147047)Version used: 2021-11-01T03:59:12Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.7Method: Apache HTTP Server Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.117232)

References
https://httpd.apache.org/security/vulnerabilities_22.html,https://httpd.apache.org/security/vulnerabilities_24.html

M

MEDIUM (CVSS: 4.3)

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

22/TCP (SSH)

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

Vulnerability Detection Result
The remote SSH server supports the following weak client-to-server encryption algorithm(s):3des-cbcaes128-cbcaes192-cbcaes256-cbcarcfourarcfour128arcfour256blowfish-cbccast128-cbcrijndael-cbc@lysator.liu.seThe remote SSH server supports the following weak server-to-client encryption algorithm(s):3des-cbcaes128-cbcaes192-cbcaes256-cbcarcfourarcfour128arcfour256blowfish-cbccast128-cbcrijndael-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

M

MEDIUM (CVSS: 4.3)

NVT: OPENSSH SECURITY BYPASS VULNERABILITY (OID: 1.3.6.1.4.1.25623.1.0.806049)

22/TCP (SSH)

Summary
OpenSSH is prone to a security bypass vulnerability.

Vulnerability Detection Result
Installed version: 6.6.1p1Fixed version: 6.9Installationpath / 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

M

MEDIUM (CVSS: 4.3)

NVT: APACHE HTTP SERVER MOD_CACHE DENIAL OF SERVICE VULNERABILITY -01 MAY15 (OID: 1.3.6.1.4.1.25623.1.0.805635)

80/TCP (HTTP)

Summary
Apache HTTP Server is prone to a denial of service vulnerability.

Vulnerability Detection Result
Installed version: 2.4.7Fixed version: 2.4.10Installationpath / port: 80/tcp

Impact
Successful exploitation will allow a remote attacker to cause a denial of service via a crafted HTTP Connection header when a reverse proxy is enabled.

Solution
Update to version 2.4.10 or later.

Vulnerability Insight
Flaw is due to vulnerability in mod_proxy module in the Apache HTTP Server.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:Apache HTTP Server 'mod_cache' Denial of Service Vulnerability -01 May15(OID: 1.3.6.1.4.1.25623.1.0.805635)Version used: 2022-04-14T06:42:08Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.7Method: Apache HTTP Server Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.117232)

References
http://zerodayinitiative.com/advisories/ZDI-14-239/,http://httpd.apache.org/security/vulnerabilities_24.html

M

MEDIUM (CVSS: 4.3)

NVT: APACHE HTTP SERVER MOD_LUA DENIAL OF SERVICE VULNERABILITY MAY15 (OID: 1.3.6.1.4.1.25623.1.0.805637)

80/TCP (HTTP)

Summary
Apache HTTP Server is prone to a denial of service vulnerability.

Vulnerability Detection Result
Installed version: 2.4.7Fixed version: 2.4.12Installationpath / port: 80/tcp

Impact
Successful exploitation will allow a remote attacker to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives.

Solution
Update to version 2.4.12 or later.

Vulnerability Insight
Flaw is due to a vulnerability in LuaAuthzProvider that is triggered if a user-supplied LUA script is supplied more than once with different arguments.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.Details:Apache HTTP Server 'mod_lua' Denial of Service Vulnerability May15(OID: 1.3.6.1.4.1.25623.1.0.805637)Version used: 2022-04-14T06:42:08Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.4.7Method: Apache HTTP Server Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.117232)

References
http://httpd.apache.org/security/vulnerabilities_24.html,http://www.rapid7.com/db/vulnerabilities/apache-httpd-cve-2014-8109

L

LOW (CVSS: 2.6)

NVT: TCP TIMESTAMPS (OID: 1.3.6.1.4.1.25623.1.0.80091)

0/NA

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

Vulnerability Detection Result
It was detected that the host implements RFC1323/RFC7323.The following timestamps were retrieved with a delay of 1 seconds in-between:Packet 1: 1936300982Packet 2: 1936302131

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

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

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

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

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

L	LOW (CVSS: 2.6) NVT: WEAK MAC ALGORITHM(S) SUPPORTED (SSH) (OID: 1.3.6.1.4.1.25623.1.0.105610)	22/TCP (SSH)

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

Vulnerability Detection Result
The remote SSH server supports the following weak client-to-server MAC algorithm(s):hmac-md5hmac-md5-96hmac-md5-96-etm@openssh.comhmac-md5-etm@openssh.comhmac-sha1-96hmac-sha1-96-etm@openssh.comThe remote SSH server supports the following weak server-to-client MAC algorithm(s):hmac-md5hmac-md5-96hmac-md5-96-etm@openssh.comhmac-md5-etm@openssh.comhmac-sha1-96hmac-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