



VulScan

External Vulnerability Scan Issues Report



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

01 | Summary

02 | Details

[2.1 Apache HTTP Server 2.4.0 - 2.4.46 Multiple Vulnerabilities - Linux](#)

[2.2 Apache HTTP Server Multiple Vulnerabilities Apr18 \(Linux\)](#)

[2.3 Apache HTTP Server < 2.4.49 Multiple Vulnerabilities - Linux](#)

[2.4 Apache HTTP Server Multiple Vulnerabilities June17 \(Linux\)](#)

[2.5 Apache HTTP Server <= 2.4.51 Buffer Overflow Vulnerability - Linux](#)

[2.6 Apache HTTP Server mod_auth_digest Multiple Vulnerabilities \(Linux\)](#)

[2.7 OpenSSH Multiple Vulnerabilities](#)

[2.8 Apache HTTP Server 2.4.7 - 2.4.51 Multiple Vulnerabilities - Linux](#)

[2.9 OpenSSH Client Information Leak](#)

[2.10 Apache HTTP Server Man-in-the-Middle Attack Vulnerability - July16 \(Linux\)](#)

[2.11 OpenSSH Privilege Escalation Vulnerability - May16](#)

[2.12 Apache HTTP Server OPTIONS Memory Leak Vulnerability \(Optionsbleed\) - Version Check](#)

[2.13 OpenSSH Denial of Service And User Enumeration Vulnerabilities \(Linux\)](#)

[2.14 Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability \(SSH, D\(HE\)ater\)](#)

[2.15 Apache HTTP Server Denial of Service Vulnerability-02 Apr18 \(Linux\)](#)

[2.16 Apache HTTP Server mod_auth_digest DoS Vulnerability \(Linux\)](#)

[2.17 Apache HTTP Server mod_session_crypto Vulnerability \(Dec 2016\) - Linux](#)

[2.18 Apache HTTP Server < 2.4.39 mod_auth_digest Access Control Bypass Vulnerability \(Linux\)](#)

- 2.19 Apache HTTP Server < 2.4.38 mod_session_cookie Vulnerability (Linux)
- 2.20 Apache HTTP Server < 2.4.48 NULL Pointer Dereference Vulnerability - Linux
- 2.21 OpenSSH Multiple Vulnerabilities Jan17 (Linux)
- 2.22 OpenSSH 6.2 <= 8.7 Privilege Escalation Vulnerability
- 2.23 Apache HTTP Server Multiple Vulnerabilities (Sep 2014) - Linux
- 2.24 Apache HTTP Server Multiple Vulnerabilities May15
- 2.25 OpenSSH <= 7.2p1 - Xauth Injection
- 2.26 Apache HTTP Server 2.4.0 < 2.4.42 Multiple Vulnerabilities (Linux)
- 2.27 Apache HTTP Server CRLF Injection Vulnerability (Dec 2016) - Linux
- 2.28 Apache HTTP Server 2.4.0 - 2.4.40 Multiple Vulnerabilities (Linux)
- 2.29 OpenBSD OpenSSH <= 7.9 Multiple Vulnerabilities
- 2.30 OpenBSD OpenSSH Information Disclosure Vulnerability (CVE-2020-14145)
- 2.31 OpenSSH sftp-server Security Bypass Vulnerability (Linux)
- 2.32 Weak Host Key Algorithm(s) (SSH)
- 2.33 Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)
- 2.34 OpenSSH Denial of Service Vulnerability - Jan16
- 2.35 Apache HTTP Server 2.4.1 < 2.4.24 IP Spoofing Vulnerability (Linux)
- 2.36 Apache HTTP Server < 2.4.39 URL Normalization Vulnerability (Linux)
- 2.37 Apache HTTP Server 2.4.6 - 2.4.46 Tunneling Misconfiguration Vulnerability - Linux
- 2.38 OpenSSH auth2-gss.c User Enumeration Vulnerability - Linux
- 2.39 OpenSSH Information Disclosure Vulnerability (CVE-2016-20012)
- 2.40 OpenSSH < 7.8 User Enumeration Vulnerability - Linux
- 2.41 Apache HTTP Server <= 2.4.52 Multiple Vulnerabilities - Linux
- 2.42 Apache HTTP Server Multiple Vulnerabilities (Mar 2014) - Linux
- 2.43 Apache HTTP Server Multiple Vulnerabilities August15 (Linux)



2.44 Apache HTTP Server mod_lua Denial of Service Vulnerability -01 May15

2.45 Apache HTTP Server DoS Vulnerability (Sep 2014) - Linux

2.46 Enabled Directory Listing Detection

2.47 Weak Encryption Algorithm(s) Supported (SSH)

2.48 Apache HTTP Server mod_lua Denial of Service Vulnerability May15

2.49 OpenSSH Security Bypass Vulnerability

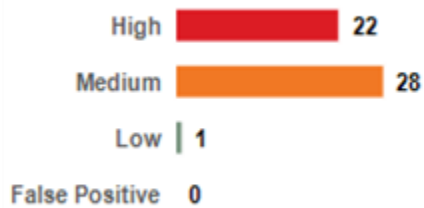
2.50 Apache HTTP Server mod_cache Denial of Service Vulnerability -01 May15

2.51 Weak MAC Algorithm(s) Supported (SSH)

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: External

Components Scanned

IP Address	Hostname	MAC Address
45.33.32.156	(96-68-119-142-static.atl.earthlink.net)	

2 - Scan Details

2.1 - Apache HTTP Server 2.4.0 - 2.4.46 Multiple Vulnerabilities - Linux

H

HIGH: (CVSS: 9.8)

OID: 1.3.6.1.4.1.25623.1.0.112897

80/TCP
(HTTP)

Summary

Apache HTTP Server is prone to multiple vulnerabilities.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

Installed version: 2.4.7 Fixed version: 2.4.48 Installation path / port: 80/tcp

Impact

- CVE-2020-35452: A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. - CVE-2021-26690: A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service. - CVE-2021-26691: A specially crafted SessionHeader sent by an origin server could cause a heap overflow.

Solution

Update to version 2.4.48 or later.

Vulnerability Insight

The following vulnerabilities exist: - CVE-2020-35452: mod_auth_digest possible stack overflow by one null byte - CVE-2021-26690: mod_session NULL pointer dereference - CVE-2021-26691: mod_session response handling heap overflow

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host. Details: Apache HTTP Server 2.4.0 - 2.4.46 Multiple Vulnerabilities - Linux(OID: 1.3.6.1.4.1.25623.1.0.112897) Version used: 2021-08-24T09:01:06Z

Product Detection Result

Product: cpe:/a:apache:http_server:2.4.7 Method: 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

2.2 - Apache HTTP Server Multiple Vulnerabilities Apr18 (Linux)

H

HIGH: (CVSS: 9.8)

OID: 1.3.6.1.4.1.25623.1.0.812844

80/TCP
(HTTP)



Summary

Apache HTTP Server is prone to multiple vulnerabilities.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

Installed version: 2.4.7 Fixed version: 2.4.30 Installation path / port: 80/tcp

Impact

Successful exploitation will allow an attacker to replay HTTP requests across servers without detection, influence the user content, upload a malicious file, crash the Apache HTTP Server and perform denial of service attack.

Solution

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

Vulnerability Insight

Multiple flaws exist due to: - Apache HTTP Server fails to correctly generate the nonce sent to prevent replay attacks. - Misconfigured mod_session variable, HTTP_SESSION. - Apache HTTP Server fails to sanitize the expression specified in '<FilesMatch>'. - An error in Apache HTTP Server 'mod_authnz_ldap' when configured with AuthLDAPCharsetConfig. - Apache HTTP Server fails to sanitize against a specially crafted request.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host. Details: Apache HTTP Server Multiple Vulnerabilities Apr18 (Linux)(OID: 1.3.6.1.4.1.25623.1.0.812844) Version used: 2021-06-15T02:00:29Z

Product Detection Result

Product: cpe:/a:apache:http_server:2.4.7 Method: 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

2.3 - Apache HTTP Server < 2.4.49 Multiple Vulnerabilities - Linux



HIGH: (CVSS: 9.8)

OID: 1.3.6.1.4.1.25623.1.0.146725

80/TCP
(HTTP)

Summary

Apache HTTP Server is prone to multiple vulnerabilities.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

Installed version: 2.4.7 Fixed version: 2.4.49 Installation path / port: 80/tcp

Solution

Update to version 2.4.49 or later.

Vulnerability Insight

The following vulnerabilities exist: - CVE-2021-34798: NULL pointer dereference in httpd core - CVE-2021-39275: ap_escape_quotes buffer overflow - CVE-2021-40438: mod_proxy SSRF

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host. Details: Apache HTTP Server < 2.4.49 Multiple Vulnerabilities -



Linux(OID: 1.3.6.1.4.1.25623.1.0.146725)Version used: 2021-09-29T08:01:30Z

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

2.4 - Apache HTTP Server Multiple Vulnerabilities June17 (Linux)



HIGH: (CVSS: 9.8)

OID: 1.3.6.1.4.1.25623.1.0.811214

80/TCP
(HTTP)

Summary

Apache HTTP Server is prone to multiple vulnerabilities.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

Installed version: 2.4.7 Fixed version: 2.4.26 Installation path / port: 80/tcp

Impact

Successful exploitation will allow remote attackers to bypass authentication and perform unauthorized actions, cause a denial-of-service condition and gain access to potentially sensitive information.

Solution

Update to Apache HTTP Server 2.2.33 or 2.4.26 or later.

Vulnerability Insight

Multiple flaws exist as, - The mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header. - The mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port. - An use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.Details:Apache HTTP Server Multiple Vulnerabilities June17 (Linux)(OID: 1.3.6.1.4.1.25623.1.0.811214)Version used: 2021-09-14T08:01:37Z

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://seclists.org/oss-sec/2017/q2/509>,http://httpd.apache.org/security/vulnerabilities_24.html,http://httpd.apache.org/security/vulnerabilities_22.html

2.5 - Apache HTTP Server <= 2.4.51 Buffer Overflow Vulnerability - Linux



HIGH: (CVSS: 9.8)

OID: 1.3.6.1.4.1.25623.1.0.117856

80/TCP
(HTTP)

Summary

Apache HTTP Server is prone to a buffer overflow vulnerability.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

Installed version: 2.4.7 Fixed version: 2.4.52 Installation path / port: 80/tcp

Solution

Update to version 2.4.52 or later.

Vulnerability Insight

A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts).

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host. Details: Apache HTTP Server <= 2.4.51 Buffer Overflow Vulnerability - Linux (OID: 1.3.6.1.4.1.25623.1.0.117856) Version used: 2021-12-23T12:12:57Z

Product Detection Result

Product: cpe:/a:apache:http_server:2.4.7 Method: 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

2.6 - Apache HTTP Server mod_auth_digest Multiple Vulnerabilities (Linux)



HIGH: (CVSS: 9.1)

OID: 1.3.6.1.4.1.25623.1.0.811237

80/TCP
(HTTP)

Summary

Apache HTTP Server is prone to multiple vulnerabilities.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

Installed version: 2.4.7 Fixed version: 2.4.27 Installation path / port: 80/tcp

Impact

Successful exploitation will allow remote attackers to cause the target service to crash. A remote user can obtain potentially sensitive information as well on the target system.

Solution

Update to Apache HTTP Server 2.2.34 or 2.4.27 or later.

Vulnerability Insight

The flaw exists due to error in Apache 'mod_auth_digest' which does not properly initialize memory used to process 'Digest' type HTTP Authorization headers.



Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.Details:Apache HTTP Server 'mod_auth_digest' Multiple Vulnerabilities (Linux)(OID: 1.3.6.1.4.1.25623.1.0.811237)Version used: 2021-09-08T14:01:33Z

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.securitytracker.com/id/1038906>,http://httpd.apache.org/security/vulnerabilities_22.html,http://httpd.apache.org/security/vulnerabilities_24.html

2.7 - OpenSSH Multiple Vulnerabilities

H

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: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

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>

2.8 - Apache HTTP Server 2.4.7 - 2.4.51 Multiple Vulnerabilities - Linux

H

HIGH: (CVSS: 8.2)

OID: 1.3.6.1.4.1.25623.1.0.117854

80/TCP
(HTTP)



Summary

Apache HTTP Server is prone to multiple vulnerabilities.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

Installed version: 2.4.7 Fixed version: 2.4.52 Installation path / 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: 2021-12-23T12:12:5Z

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

2.9 - OpenSSH Client Information Leak



HIGH: (CVSS: 8.1)

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.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

Installed version: 6.6.1p1 Fixed version: 7.1p2 Installation path / 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>

2.10 - Apache HTTP Server Man-in-the-Middle Attack Vulnerability - July16 (Linux)



HIGH: (CVSS: 8.1)

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.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

Installed version: 2.4.7 Fixed version: 2.4.24 Installation path / 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: 2021-10-12T12:01:25Z

Product Detection Result

Product: cpe:/a:apache:http_server:2.4.7 Method: 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>

2.11 - OpenSSH Privilege Escalation Vulnerability - May16



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: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)



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:6.6.1p1 Method: 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>

2.12 - Apache HTTP Server OPTIONS Memory Leak Vulnerability (Optionsbleed) - Version Check

H

HIGH: (CVSS: 7.5)

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.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

Installed version: 2.4.7 Fixed version: 2.4.28 Installation path / 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 completely via the 'AllowOverride None' directive within the webserver's 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: 2021-09-13T11:01:38Z

Product Detection Result

Product: cpe:/a:apache:http_server:2.4.7 Method: 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

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



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: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

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:6.6.1p1 Method: 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>

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

PAGE 14 OF 39



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: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

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>

2.15 - Apache HTTP Server Denial of Service Vulnerability-02 Apr18 (Linux)



HIGH: (CVSS: 7.5)

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.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

Installed version: 2.4.7 Fixed version: 2.4.30 Installation path / 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: 2021-06-15T02:00:29Z

Product Detection Result

Product: cpe:/a:apache:http_server:2.4.7 Method: 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

2.16 - Apache HTTP Server mod_auth_digest DoS Vulnerability (Linux)



HIGH: (CVSS: 7.5)

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.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

Installed version: 2.4.7 Fixed version: 2.4.25 Installation path / 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: 2021-09-13T11:01:38Z

Product Detection Result

Product: cpe:/a:apache:http_server:2.4.7 Method: 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

2.17 - Apache HTTP Server mod_session_crypto Vulnerability (Dec 2016) - Linux



HIGH: (CVSS: 7.5)

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.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

Installed version: 2.4.7 Fixed version: 2.4.25 Installation path / 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:2.4.7 Method: 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

2.18 - Apache HTTP Server < 2.4.39 mod_auth_digest Access Control Bypass Vulnerability (Linux)



HIGH: (CVSS: 7.5)

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.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

Installed version: 2.4.7 Fixed version: 2.4.39 Installation path / 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

2.19 - Apache HTTP Server < 2.4.38 mod_session_cookie Vulnerability (Linux)

HIGH: (CVSS: 7.5)

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.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

Installed version: 2.4.7 Fixed version: 2.4.38 Installation path / 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

2.20 - Apache HTTP Server < 2.4.48 NULL Pointer Dereference Vulnerability - Linux

HIGH: (CVSS: 7.5)

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.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)



Vulnerability Detection Result

Installed version: 2.4.7 Fixed version: 2.4.48 Installation path / 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:2.4.7 Method: 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

2.21 - OpenSSH Multiple Vulnerabilities Jan17 (Linux)



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: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

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 serial-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:6.6.1p1 Method: 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>

2.22 - 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 escalation vulnerability in certain configurations.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

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:6.6.1p1 Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References

<https://www.openssh.com/txt/release-8.8>

2.23 - Apache HTTP Server Multiple Vulnerabilities (Sep 2014) - Linux

M

MEDIUM: (CVSS: 6.8)

OID: 1.3.6.1.4.1.25623.1.0.147048

80/TCP
(HTTP)

Summary



Apache HTTP Server is prone to multiple vulnerabilities.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

Installed version: 2.4.7 Fixed version: 2.4.12 Installation path / 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:2.4.7 Method: 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

2.24 - Apache HTTP Server Multiple Vulnerabilities May15

M

MEDIUM: (CVSS: 6.8)

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.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

Installed version: 2.4.7 Fixed version: 2.4.10 Installation path / 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: 2021-03-01T08:21:56Z

Product Detection Result

Product: cpe:/a:apache:http_server:2.4.7 Method: 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>

2.25 - OpenSSH <= 7.2p1 - Xauth Injection

M

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: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

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:6.6.1p1 Method: OpenSSH Detection Consolidation(OID: 1.3.6.1.4.1.25623.1.0.108577)

References

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

2.26 - Apache HTTP Server 2.4.0 < 2.4.42 Multiple Vulnerabilities (Linux)

M

MEDIUM: (CVSS: 6.1)
OID: 1.3.6.1.4.1.25623.1.0.143671

80/TCP
(HTTP)

Summary

Apache HTTP Server is prone to multiple vulnerabilities.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

Installed version: 2.4.7 Fixed version: 2.4.42 Installation path / 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

2.27 - Apache HTTP Server CRLF Injection Vulnerability (Dec 2016) - Linux

M

MEDIUM: (CVSS: 6.1)
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.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

Installed version: 2.4.7 Fixed version: 2.4.25 Installation path / 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:2.4.7 Method: 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

2.28 - Apache HTTP Server 2.4.0 - 2.4.40 Multiple Vulnerabilities (Linux)

M

MEDIUM: (CVSS: 6.1)

OID: 1.3.6.1.4.1.25623.1.0.114143

80/TCP
(HTTP)

Summary

Apache HTTP Server is prone to multiple vulnerabilities.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

Installed version: 2.4.7 Fixed version: 2.4.41 Installation path / 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:2.4.7 Method: 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

2.29 - OpenBSD OpenSSH <= 7.9 Multiple Vulnerabilities

M

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: External**

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

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>

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

M

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: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

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>

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

M

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: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

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:6.6.1p1 Method: 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>

2.32 - 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: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

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

2.33 - 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: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

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>

2.34 - OpenSSH Denial of Service Vulnerability - Jan16

M	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: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

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>

2.35 - Apache HTTP Server 2.4.1 < 2.4.24 IP Spoofing Vulnerability (Linux)

M

MEDIUM: (CVSS: 5.3)

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.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

Installed version: 2.4.7 Fixed version: 2.4.24 Installation path / 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

2.36 - Apache HTTP Server < 2.4.39 URL Normalization Vulnerability (Linux)

M

MEDIUM: (CVSS: 5.3)

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.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

Installed version: 2.4.7 Fixed version: 2.4.39 Installation path / 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:2.4.7 Method: 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

2.37 - Apache HTTP Server 2.4.6 - 2.4.46 Tunneling Misconfiguration Vulnerability - Linux

M

MEDIUM: (CVSS: 5.3)

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.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

Installed version: 2.4.7 Fixed version: 2.4.48 Installation path / 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

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

M

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: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

Installed version: 6.6.1p1 Fixed version: None Installation path / port: 22/tcp

Impact

Successful 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-gss.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>

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

PAGE 30 OF 39

PROPRIETARY & CONFIDENTIAL

M

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: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

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:6.6.1p1 Method: 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>

2.40 - OpenSSH < 7.8 User Enumeration Vulnerability - Linux

M

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: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

Installed version: 6.6.1p1 Fixed version: 7.8 Installation path / port: 22/tcp

Impact

Successful 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>

2.41 - Apache HTTP Server <= 2.4.52 Multiple Vulnerabilities - Linux

M

MEDIUM: (CVSS: 5)

OID: 1.3.6.1.4.1.25623.1.0.113837

80/TCP
(HTTP)

Summary

Apache HTTP Server is prone to multiple vulnerabilities.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

Installed version: 2.4.7 Fixed version: 2.4.53 Installation path / 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: 2022-03-14T15:53:09Z

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)

2.42 - Apache HTTP Server Multiple Vulnerabilities (Mar 2014) - Linux

M

MEDIUM: (CVSS: 5)

OID: 1.3.6.1.4.1.25623.1.0.147047

80/TCP
(HTTP)



Summary

Apache HTTP Server is prone to multiple vulnerabilities.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

Installed version: 2.4.7 Fixed version: 2.4.9 Installation path / 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:2.4.7 Method: 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

2.43 - Apache HTTP Server Multiple Vulnerabilities August15 (Linux)

M

MEDIUM: (CVSS: 5)

OID: 1.3.6.1.4.1.25623.1.0.806018

80/TCP
(HTTP)

Summary

Apache HTTP Server is prone to multiple vulnerabilities.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

Installed version: 2.4.7 Fixed version: 2.4.14 Installation path / 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: 2021-03-01T08:21:56Z

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

2.44 - Apache HTTP Server mod_lua Denial of Service Vulnerability -01 May15



MEDIUM: (CVSS: 5)

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.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

Installed version: 2.4.7 Fixed version: 2.4.13 Installation path / 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: 2021-03-01T08:21:56Z

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>

2.45 - Apache HTTP Server DoS Vulnerability (Sep 2014) - Linux



MEDIUM: (CVSS: 5)

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.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

Installed version: 2.4.7 Fixed version: 2.4.12 Installation path / port: 80/tcp

Solution

Update to version 2.4.12 or later.

Vulnerability Insight

A NULL pointer dereference 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:2.4.7 Method: 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

2.46 - Enabled Directory Listing Detection

M

MEDIUM: (CVSS: 5)

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.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

The following directories with an enabled directory listing were identified: <http://scanme.nmap.org/shared>
<http://scanme.nmap.org/shared/error> <http://scanme.nmap.org/shared/error/includes> <http://scanme.nmap.org/shared/templates>
Please 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 webserver's 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

2.47 - 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: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

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 algorithms
Details: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>

2.48 - Apache HTTP Server mod_lua Denial of Service Vulnerability May15

M

MEDIUM: (CVSS: 4.3)

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.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

Installed version: 2.4.7 Fixed version: 2.4.12 Installation path / 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: 2021-03-01T08:21:56Z

Product Detection Result

Product: cpe:/a:apache:http_server:2.4.7 Method: 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>

2.49 - OpenSSH Security Bypass Vulnerability

M

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: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

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:6.6.1p1 Method: 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>

2.50 - Apache HTTP Server mod_cache Denial of Service Vulnerability -01 May15

M

MEDIUM: (CVSS: 4.3)

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.

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

Vulnerability Detection Result

Installed version: 2.4.7 Fixed version: 2.4.10 Installation path / 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: 2021-03-01T08:21:56Z

Product Detection Result

Product: cpe:/a:apache:http_server:2.4.7 Method: 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

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

L

LOW: (CVSS: 2.6)

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).

Affected Nodes: External

96.68.119.142 (96-68-119-142-static.atl.earthlink.net)

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 algorithm Details: Weak MAC



Algorithm(s) Supported (SSH)(OID: 1.3.6.1.4.1.25623.1.0.105610)Version used: 2021-09-20T11:05:40Z
