NIST

☰ NVD MENU

NATIONAL VULNERABILITY DATABASE

NIST NATIONAL VULNERABILITY DATABASE NVD

VULNERABILITIES

CVE-2021-41773 Detail

Description

A flaw was found in a change made to path normalization in Apache HTTP Server 2.4.49. An attacker could use a path traversal attack to outside the directories configured by Alias-like directives. If files outside of these directories are not protected by the usual default configu denied", these requests can succeed. If CGI scripts are also enabled for these aliased pathes, this could allow for remote code execution. T exploited in the wild. This issue only affects Apache 2.4.49 and not earlier versions. The fix in Apache HTTP Server 2.4.50 was found to be in 2021-42013.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displa

CVSS 3.x Severity and Vector Strings:

NIST: NVD **Base Score:** 7.5 HIGH

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have inform be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be othe are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on the NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd

Hyperlink
http://packetstormsecurity.com/files/164418/Apache-HTTP-Server-2.4.49-Path-Traversal-Remote-Code-Execution.html
http://packetstormsecurity.com/files/164418/Apache-HTTP-Server-2.4.49-Path-Traversal.html

http://packetstormsecurity.com/files/164629/Apache-2.4.49-2.4.50-Traversal-Remote-Code-Execution.html
http://packetstormsecurity.com/files/164941/Apache-HTTP-Server-2.4.50-Remote-Code-Execution.html
http://www.openwall.com/lists/oss-security/2021/10/05/2
http://www.openwall.com/lists/oss-security/2021/10/07/1
http://www.openwall.com/lists/oss-security/2021/10/07/6
http://www.openwall.com/lists/oss-security/2021/10/08/1
http://www.openwall.com/lists/oss-security/2021/10/08/2
http://www.openwall.com/lists/oss-security/2021/10/08/3
http://www.openwall.com/lists/oss-security/2021/10/08/4
http://www.openwall.com/lists/oss-security/2021/10/08/5
http://www.openwall.com/lists/oss-security/2021/10/08/6
http://www.openwall.com/lists/oss-security/2021/10/09/1
http://www.openwall.com/lists/oss-security/2021/10/11/4
http://www.openwall.com/lists/oss-security/2021/10/15/3
http://www.openwall.com/lists/oss-security/2021/10/16/1
https://httpd.apache.org/security/vulnerabilities_24.html

https://lists.apache.org/thread.html/r17a4c6ce9aff662efd9459e9d1850ab4a611cb23392fc68264c72cb3%40%3Ccvs.httpd.apache.org%3E
https://lists.apache.org/thread.html/r6abf5f2ba6f1aa8b1030f95367aaf17660c4e4c78cb2338aee18982f%40%3Cusers.httpd.apache.org%3E
https://lists.apache.org/thread.html/r7c795cd45a3384d4d27e57618a215b0ed19cb6ca8eb070061ad5d837%40%3Cannounce.apache.org%3E
https://lists.apache.org/thread.html/r98d704ed4377ed889d40479db79ed1ee2f43b2ebdd79ce84b042df45%40%3Cannounce.apache.org%3E
https://lists.apache.org/thread.html/rb5b0e46f179f60b0c70204656bc52fcb558e961cb4d06a971e9e3efb%40%3Cusers.httpd.apache.org%3E
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/RMIIEFINL6FUIOPD2A3M5XC6DH45Y3CC/
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/WS5RVHOIIRECG65ZBTZY7IEJVWQSQPG3/
https://security.gentoo.org/glsa/202208-20
https://security.netapp.com/advisory/ntap-20211029-0009/
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-httpd-pathtrv-LAzg68cZ
https://www.oracle.com/security-alerts/cpujan2022.html

This CVE is in CISA's Known Exploited Vulnerabilities Catalog

Reference CISA's BOD 22-01 and Known Exploited Vulnerabilities Catalog for further guidance and requirements.

Vulnerability Name	Date Added	Due Date	Required Action
Apache HTTP Server Path Traversal Vulnerability	11/03/2021	11/17/2021	Apply updates per vendor instr

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	NIST Apache Software Fou

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:a:apache:http_server:2.4.49:*:*:*:*:*:*:*
Show Matching CPE(s)▾

Configuration 2 (hide)

cpe:2.3:o:fedoraproject:fedora:34:*:*:*:*:*:*:*
Show Matching CPE(s)▾

cpe:2.3:o:fedoraproject:fedora:35:*:*:*:*:*:*:*
Show Matching CPE(s)▾

Configuration 3 (hide)

cpe:2.3:a:oracle:instantis_enterprisetrack:17.1:*:*:*:*:*:*:*
Show Matching CPE(s)▾

cpe:2.3:a:oracle:instantis_enterprisetrack:17.2:*:*:*:*:*:*:*
Show Matching CPE(s)▾

cpe:2.3:a:oracle:instantis_enterprisetrack:17.3:*:*:*:*:*:*:*
Show Matching CPE(s)▾

Configuration 4 (hide)

cpe:2.3:a:netapp:cloud_backup:-:*:*:*:*:*:*:*

Show Matching CPE(s)▾

Denotes Vulnerable Software

Are we missing a CPE here? Please let us know.

Change History

32 change records found show changes

QUICK INFO

CVE Dictionary Entry:

CVE-2021-41773

NVD Published Date:

10/05/2021

NVD Last Modified:

07/26/2024

Source:

Apache Software Foundation

NIST
NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

HEADQUARTERS
100 Bureau Drive
Gaithersburg, MD 20899
(301) 975-2000

Webmaster | Contact Us | Our Other Offices

Incident Response Assistance and Non-NVD Related
Technical Cyber Security Questions:
US-CERT Security Operations Center
Email: soc@us-cert.gov
Phone: 1-888-282-0870

Site Privacy | Accessibility | Privacy Program | Copyrights | Vulnerability Disclosure | No Fear Act Policy | FOIA | Environmental Policy | Scientific Integrity | Information Quality Standards | Commerce.gov | Science.gov | USA.gov