

CVE-2021-41773

Apache HTTP Server Path Traversal Vulnerability

Exigent CISA KEV since Nov 3, 2021 Actively exploited Ransomware use known Public exploit module (Metasploit)

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 map URLs to files outside the directories configured by Alias-like directives. If files outside of these directories are not protected by the usual default configuration "require all denied", these requests can succeed. If CGI scripts are also enabled for these aliased pathes, this could allow for remote code execution. This issue is known to be exploited in the wild.

EVRS 94/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.999 99.99th percentile · FIRST	CISA DEADLINE Nov 17, 2021 KEV since 2021 · listed over a year
--	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☒ Ransomware	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.999 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

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 incomplete, see CVE-2021-42013.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
http server	2.4.49	no fixed version listed	NVD
instantis enterprisetrack	17.1 17.2 17.3	no fixed version listed	NVD
cloud backup	—	no fixed version listed	NVD
fedora	34 35	no fixed version listed	NVD

Sources

Vendor guidance	lists.apache.org/thread.html/r17a4c6ce9aff662efd9459e9d1850ab4a611cb23392fc68264c72cb3%40%3Ccvss.httpd.apache.org%3Envd.nist.gov/vuln/detail/CVE-2021-41773	Additional guidance	httpd.apache.org/security/vulnerabilities_24.html
NVD	nvd.nist.gov/vuln/detail/CVE-2021-41773	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2021-28781	Current data	evulnable.com/vulnerability-management/cve/CVE-2021-41773

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.