

CVE-2021-40438

Apache HTTP Server-Side Request Forgery (SSRF)

Exigent

CISA KEV since Dec 1, 2021

Actively exploited

Ransomware use known

A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

EVRS 93 /100 Immediate priority	CVSS V3.1 9.0 Critical · NVD	EPSS 0.999 99.99th percentile · FIRST	CISA DEADLINE Dec 15, 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 9.0	☐ 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

Affected and fixed versions · 31 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
jboss core services	1.0	no fixed version listed	NVD
software collections	1.0	no fixed version listed	NVD
http server	≤ 2.4.48 12.2.1.3.0 12.2.1.4.0	no fixed version listed	NVD
cloud backup	–	no fixed version listed	NVD
clustered data ontap	–	no fixed version listed	NVD
storagegrid	–	no fixed version listed	NVD
enterprise manager ops center	12.4.0.0	no fixed version listed	NVD
instantis enterprisetrack	17.1 17.2 17.3	no fixed version listed	NVD

Sources

Vendor guidance oracle.com/security-alerts/cpuapr2022.html

Additional guidance httpd.apache.org/security/vulnerabilities_24.html

NVD nvd.nist.gov/vuln/detail/CVE-2021-40438

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2021-27615

Current data evulnable.com/vulnerability-management/cve/CVE-2021-40438

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