

CVE-2021-25298

Nagios XI OS Command Injection

CISA KEV since Jan 18, 2022

Actively exploited

Public exploit module (Metasploit)

Nagios XI version xi-5.7.5 is affected by OS command injection. The vulnerability exists in the file `/usr/local/nagiosxi/html/includes/configwizards/cloud-vm/cloud-vm.inc.php` due to improper sanitization of authenticated user-controlled input by a single HTTP request, which can lead to OS command injection on the Nagios XI server.

EVRS 79 / ₁₀₀ Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.736 99.47th percentile · FIRST	CISA DEADLINE Feb 1, 2022 KEV since 2022 · 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	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.736 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
nagios xi	≥ 5.5.6 ≤ 5.7.5	after 5.7.5	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-6gq5-wx57-577c	NVD	nvd.nist.gov/vuln/detail/CVE-2021-25298
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2021-12198
Current data	evulnable.com/vulnerability-management/cve/CVE-2021-25298		

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