CVE-2021-25297

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2021-25297
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-02-15 13:15:00 UTC
Updated	2023-08-08 14:21:00 UTC
Description	Nagios XI version xi-5.7.5 is affected by OS command injection. The vulnerability exists in the file /usr/local/nagiosxi/html/in

Risk And Classification

EPSS: 0.818750000 probability, percentile 0.992130000 (date 2026-05-12)

CISA KEV: Listed on 2022-01-18; due 2022-02-01; ransomware use Unknown

Problem Types: NVD-CWE-Other

CISA Known Exploited Vulnerability

Vendor	Nagios
Product	Nagios XI
Name	Nagios XI OS Command Injection
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2021-25297

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nagios	Nagios Xi	5.7.5	All	All	All
Application	Nagios	Nagios Xi	5.7.5	All	All	All

References

Reference	Source	Link
Nagios - Network, Server and Log Monitoring Software	MISC	nagios.com
nagios-xi-5.7.5-bugs/README.md at main · fs0c-sh/nagios-xi-5.7.5-bugs · GitHub	MISC	github.com
Nagios XI · Previous Versions	MISC	assets.nagios.com

Nagios XI 5.7.5 Remote Code Execution ≈ Packet Storm	MISC	packetstormsecuri
Anatomy of a Command Injection: CVE-2021-25296(7,8) with Metasploit Module & Nuclei Template | Fastly	MISC	www.fastly.com
Nagios XI 5.7.5 Remote Code Execution ≈ Packet Storm	MISC	packetstormsecuri
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

375516 Nagios XI 5.7.5 Have Multiple Vulnerabilities

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**