CVE-2019-15949

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

Summary

CVE	CVE-2019-15949
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-09-05 17:15:00 UTC
Updated	2021-04-15 21:16:00 UTC
Description	Nagios XI before 5.6.6 allows remote command execution as root. The exploit requires access to the server as the nagios u

Risk And Classification

EPSS: 0.870530000 probability, percentile 0.994460000 (date 2026-05-02)

CISA KEV: Listed on 2021-11-03; due 2022-05-03; ransomware use Unknown

Problem Types: CWE-78

CISA Known Exploited Vulnerability

Vendor	Nagios
Product	Nagios XI
Name	Nagios XI Remote Code Execution Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2019-15949

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
GitHub - jakgibb/nagiosxi-root-rce-exploit: POC which exploits a vulnerability within Nagios XI (5.6.5) to spawn a root shell	MISC	githu
Nagios XI getprofile.sh Remote Command Execution ≈ Packet Storm	MISC	pack
Nagios XI Authenticated Remote Command Execution ≈ Packet Storm	MISC	pack

CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.
CISA Known Exploited Vulnerabilities catalog	CISA	www

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.