CVE-2020-35269

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-35269
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-23 19:15:00 UTC
Updated	2021-03-02 21:15:00 UTC
Description	Nagios Core application version 4.2.4 is vulnerable to Site-Wide Cross-Site Request Forgery (CSRF) in many functions, like

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nagios	Nagios Core	4.2.4	All	All	All
Application	Nagios	Nagios Core	4.2.4	All	All	All

References

Reference	Source	Link	Tags
Site-Wide Cross Site Request Forgery _ Nagios Core 4.2.4 · GitHub	MISC	gist.github.com	Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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