



# CVE-2017-14312

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2017-14312
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-09-11 22:29:00 UTC
<b>Updated</b>	2019-10-03 00:03:00 UTC
<b>Description</b>	Nagios Core through 4.3.4 initially executes /usr/sbin/nagios as root but supports configuration options in which this file is o

## Risk And Classification

**Problem Types:** CWE-269

## NVD Known Affected Configurations (CPE 2.3)

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

## References

### Reference

- Nagios Core CVE-2017-14312 Local Privilege Escalation Vulnerability
- Nagios: Privilege escalation (GLSA 201812-03) — Gentoo security
- Root privilege escalation via insecure executable/config permissions (CVE-2017-14312) · Issue #424 · NagiosEnterprises/nagioscore · GitHub
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

710284 Gentoo Linux NagInternetwork Operating System Privilege escalation Vulnerability (GLSA 201812-03)

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 registered 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](#).

**CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)**