



CVE-2017-12847

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-12847
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-23 21:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	Nagios Core before 4.3.3 creates a nagios.lock PID file after dropping privileges to a non-root account, which might allow lo

Risk And Classification

Problem Types: CWE-665

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	L
nagioscore/Changelog at master · NagiosEnterprises/nagioscore · GitHub	CONFIRM	g
configure.ac: use /run/nagios.lock as the default lockfile path. · NagiosEnterprises/nagioscore@3baffa7 · GitHub	CONFIRM	g
nagios daemon should create its PID file before dropping privileges · Issue #404 · NagiosEnterprises/nagioscore · GitHub	CONFIRM	g
halfway revert hack/configure changes - switch order of daemon_init/d... · NagiosEnterprises/nagioscore@1b19734 · GitHub	CONFIRM	g
Nagios CVE-2017-12847 Local Privilege Escalation Vulnerability	BID	v
Nagios: Multiple vulnerabilities (GLSA 201710-20) — Gentoo security	GENTOO	s
CVE Program record	CVE.ORG	v
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[710486](#) Gentoo Linux NagInternetnetwork Operating System Multiple Vulnerabilities (GLSA 201710-20)

© [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 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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)