CVE-2016-9566

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

Summary

CVE	CVE-2016-9566
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-12-15 22:59:00 UTC
Updated	2026-05-06 22:30:45 UTC
Description	base/logging.c in Nagios Core before 4.2.4 allows local users with access to an account in the nagios group to gain root pri

Risk And Classification

Primary CVSS: v3.0 7.8 HIGH from nvd@nist.gov

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.086020000 probability, percentile 0.924660000 (date 2026-05-09)

Problem Types: CWE-59 | CWE-264 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	7.2		AV:L/AC:L/Au:N/C:C/I:C/A:C

CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:L/AC:L/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
Nagios Core 4.x Version History - Nagios	af854a3a-2127-422b-91ae-364da2661
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2661
Nagios < 4.2.4 - Local Privilege Escalation - Linux local Exploit	af854a3a-2127-422b-91ae-364da2661
Full Disclosure: Nagios Core < 4.2.4 Root Privilege Escalation [CVE-2016-9566]	af854a3a-2127-422b-91ae-364da2661
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2661
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2661
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2661
Nagios 'nagios.log' File Permissions Error Lets Local Users Obtain Root Privileges - SecurityTracker	af854a3a-2127-422b-91ae-364da2661
Nagios-Exploit-Root-PrivEsc-CVE-2016-9566	af854a3a-2127-422b-91ae-364da2661

Nagios: Multiple vulnerabilities (GLSA 201702-26) — Gentoo Security	af854a3a-2127-422b-91ae-364da2661
Bug 1402869 – CVE-2016-9566 nagios: Privilege escalation issue	af854a3a-2127-422b-91ae-364da2661
[SECURITY] [DLA 1615-1] nagios3 security update	af854a3a-2127-422b-91ae-364da2661
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2661
Merge branch 'maint' · NagiosEnterprises/nagioscore@c29557d · GitHub	af854a3a-2127-422b-91ae-364da2661
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2661
Icinga: Privilege escalation (GLSA 201612-51) — Gentoo security	af854a3a-2127-422b-91ae-364da2661
Nagios: Multiple vulnerabilities (GLSA 201710-20) — Gentoo security	af854a3a-2127-422b-91ae-364da2661
Nagios CVE-2016-9566 Local Privilege Escalation Vulnerability	af854a3a-2127-422b-91ae-364da2661
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

710470 Gentoo Linux NagInternetwork Operating System Multiple Vulnerabilities (GLSA 201702-26)

710486 Gentoo Linux NagInternetwork 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 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**