



CVE-2016-8641

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

Summary

CVE	CVE-2016-8641
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-01 14:29:00 UTC
Updated	2023-02-12 23:26:00 UTC
Description	A privilege escalation vulnerability was found in nagios 4.2.x that occurs in daemon-init.in when creating necessary files and

Risk And Classification

Problem Types: CWE-59

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nagios	Nagios	4.2.0	All	All	All
Application	Nagios	Nagios	4.2.1	All	All	All
Application	Nagios	Nagios	4.2.2	All	All	All
Application	Nagios	Nagios	4.2.3	All	All	All
Application	Nagios	Nagios	4.2.0	All	All	All
Application	Nagios	Nagios	4.2.1	All	All	All
Application	Nagios	Nagios	4.2.2	All	All	All
Application	Nagios	Nagios	4.2.3	All	All	All

References

Reference	Source	Link
Nagios 4.2.2 - Local Privilege Escalation - Linux local Exploit	EXPLOIT-DB	www.exploit-db.com/exploits/41441/
github.com/NagiosEnterprises/nagioscore/commit/f2ed227673d3b2da643eb5cad...	CONFIRM	github.com
1394248 – (CVE-2016-8641) CVE-2016-8641 nagios: Unsafe ownership change leading to privilege escalation	CONFIRM	bugzilla.redhat.com/show_bug.cgi?id=1394248
Nagios CVE-2016-8641 Local Privilege Escalation Vulnerability	BID	www.securitybulletin.com/entry.php?id=1394248
Nagios: Multiple vulnerabilities (GLSA 201702-26) — Gentoo Security	GENTOO	security.gentoo.org/glsa/2017-02-26
CVE Program record	CVE.ORG	www.cve.org/CVE.explore/CVE-2016-8641

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[710470](#) Gentoo Linux NagInternetnetwork Operating System Multiple Vulnerabilities (GLSA 201702-26)

© [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](#)