



CVE-2016-6814

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2016-6814
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-01-18 18:29:00 UTC
Updated	2020-07-15 03:15:00 UTC
Description	When an application with unsupported Codehaus versions of Groovy from 1.7.0 to 2.4.3, Apache Groovy 2.4.4 to 2.4.7 on c

Risk And Classification

Problem Types: CWE-502

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Groovy	All	All	All	All
Application	Apache	Groovy	All	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All

References

Reference	Source	Link
Oracle Critical Patch Update Advisory - July 2020	MISC	www
Apache Groovy CVE-2016-6814 Remote Code Execution Vulnerability	BID	www
Red Hat Customer Portal	REDHAT	acce
Groovy: Arbitrary code execution (GLSA 202003-01) — Gentoo security	GENTOO	secu
CPU July 2018	CONFIRM	www
Oracle Critical Patch Update - April 2018	CONFIRM	www
Red Hat Customer Portal	REDHAT	acce
Red Hat Customer Portal	REDHAT	rhn.
Oracle Critical Patch Update - January 2019	CONFIRM	www
Oracle Critical Patch Update - July 2019	MISC	www

Red Hat Customer Portal	REDHAT	acce
Oracle Enterprise Manager Ops Center Networking Flaw Lets Remote Users Gain Elevated Privileges - SecurityTracker	SECTRACK	www
CPU Oct 2018	CONFIRM	www
Oracle Critical Patch Update - October 2019	MISC	www
Oracle Critical Patch Update Advisory - January 2020	MISC	www
[CVE-2016-6814] Apache Groovy Information Disclosure	MISC	mail
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.

No vendor comments have been submitted for this CVE.

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

© [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](#).

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