



CVE-2016-6489

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

Summary

CVE	CVE-2016-6489
State	PUBLIC
Assigner	security@debian.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-14 18:59:00 UTC
Updated	2020-11-16 20:20:00 UTC
Description	The RSA and DSA decryption code in Nettle makes it easier for attackers to discover private keys via a cache side channel

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.10	All	All	All
Application	Nettle Project	Nettle	All	All	All	All
Application	Nettle Project	Nettle	All	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	7.0	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
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
------------------	--------	------------------------------	-----	-----	-----	-----

References

Reference	Source	Link
Use mpz_powm_sec. (3fe1d654) · Commits · Nettle / nettle · GitLab	CONFIRM	git.lysator.liu
Red Hat Customer Portal	REDHAT	rhn.redhat.com
nettle: Information disclosure (GLSA 201706-21) — Gentoo security	GENTOO	security.gentoo.org
1362016 – (CVE-2016-6489) CVE-2016-6489 nettle: RSA/DSA code is vulnerable to cache-timing related attacks	CONFIRM	bugzilla.redhat.com
oss-security - Re: CVE Request: nettle's RSA code is vulnerable to cache sharing related attacks	MLIST	www.openwall.com
USN-3193-1: Nettle vulnerability Ubuntu	UBUNTU	www.ubuntu.com
eprint.iacr.org/2016/596.pdf	MISC	eprint.iacr.org
Oracle Critical Patch Update Advisory - April 2020	N/A	www.oracle.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

710541 Gentoo Linux nettle Information disclosure Vulnerability (GLSA 201706-21)

© 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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.cve.org). This site includes MITRE data granted under the following [license](https://www.mitre.org).

CVE.report and Source URL Uptime Status status.cve.report