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.c
nettle: Information disclosure (GLSA 201706-21) — Gentoo security	GENTOO	security.gent
1362016 – (CVE-2016-6489) CVE-2016-6489 nettle: RSA/DSA code is vulnerable to cache-timing related attacks	CONFIRM	bugzilla.redh
oss-security - Re: CVE Request: nettle's RSA code is vulnerable to cache sharing related attacks	MLIST	www.openw
USN-3193-1: Nettle vulnerability | Ubuntu	UBUNTU	www.ubuntu
eprint.iacr.org/2016/596.pdf	MISC	eprint.iacr.or
Oracle Critical Patch Update Advisory - April 2020	N/A	www.oracle.
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)