



CVE-2015-8804

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

Summary

CVE	CVE-2015-8804
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-02-23 19:59:00 UTC
Updated	2018-10-30 16:27:00 UTC
Description	x86_64/ecc-384-modp.asm in Nettle before 3.2 does not properly handle carry propagation and produces incorrect output in

Risk And Classification

Problem Types: CWE-310 | CWE-254

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Application	Nettle Project	Nettle	All	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All

References

Reference	Source
Miscalculations on secp384 curve	MLIST
openSUSE-SU-2016:0475-1: moderate: Security update for libnettle	SUSE
oss-security - Re: Miscomputations of elliptic curve scalar multiplications in Nettle	MLIST

Red Hat Customer Portal	REDHAT
ANNOUNCE: Nettle-3.2	MLIST
openSUSE-SU-2016:0486-1: moderate: Security update for libnettle	SUSE
Fix carry folding bug in x86_64 ecc_384_modp. Problem reported by Hanno Böck. (fa269b6a) · Commits · Nettle / nettle · GitLab	CONFIRM
oss-security - Miscomputations of elliptic curve scalar multiplications in Nettle	MLIST
USN-2897-1: Nettle vulnerabilities Ubuntu	UBUNTU
Miscomputations of elliptic curve scalar multiplications in Nettle The Fuzzing Project	MISC
openSUSE-SU-2016:0477-1: moderate: Security update for libnettle	SUSE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD



No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

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