# CVE-2015-8804

MITRE | NVD | CVE.ORG | Print: PDF

## 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 i |

## 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.