# CVE-2014-1959

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2014-1959 |
| **State** | PUBLIC |
| **Assigner** | cve@mitre.org |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2014-03-07 00:10:00 UTC |
| **Updated** | 2016-11-28 19:10:00 UTC |
| **Description** | lib/x509/verify.c in GnuTLS before 3.1.21 and 3.2.x before 3.2.11 treats version 1 X.509 certificates as intermediate CAs, w |

## Risk And Classification

**Problem Types:** CWE-264

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Gnu | Gnutls | 3.1.0 | All | All | All |
| Application | Gnu | Gnutls | 3.1.1 | All | All | All |
| Application | Gnu | Gnutls | 3.1.10 | All | All | All |
| Application | Gnu | Gnutls | 3.1.11 | All | All | All |
| Application | Gnu | Gnutls | 3.1.12 | All | All | All |
| Application | Gnu | Gnutls | 3.1.13 | All | All | All |
| Application | Gnu | Gnutls | 3.1.14 | All | All | All |
| Application | Gnu | Gnutls | 3.1.15 | All | All | All |
| Application | Gnu | Gnutls | 3.1.16 | All | All | All |
| Application | Gnu | Gnutls | 3.1.17 | All | All | All |
| Application | Gnu | Gnutls | 3.1.18 | All | All | All |
| Application | Gnu | Gnutls | 3.1.19 | All | All | All |
| Application | Gnu | Gnutls | 3.1.2 | All | All | All |
| Application | Gnu | Gnutls | 3.1.3 | All | All | All |
| Application | Gnu | Gnutls | 3.1.4 | All | All | All |
| Application | Gnu | Gnutls | 3.1.5 | All | All | All |
| Application | Gnu | Gnutls | 3.1.6 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Gnu | Gnutls | 3.1.7 | All | All | All |
| Application | Gnu | Gnutls | 3.1.8 | All | All | All |
| Application | Gnu | Gnutls | 3.1.9 | All | All | All |
| Application | Gnu | Gnutls | 3.2.0 | All | All | All |
| Application | Gnu | Gnutls | 3.2.1 | All | All | All |
| Application | Gnu | Gnutls | 3.2.2 | All | All | All |
| Application | Gnu | Gnutls | 3.2.3 | All | All | All |
| Application | Gnu | Gnutls | 3.2.4 | All | All | All |
| Application | Gnu | Gnutls | 3.2.5 | All | All | All |
| Application | Gnu | Gnutls | 3.2.6 | All | All | All |
| Application | Gnu | Gnutls | 3.2.7 | All | All | All |
| Application | Gnu | Gnutls | 3.2.8 | All | All | All |
| Application | Gnu | Gnutls | 3.2.8.1 | All | All | All |
| Application | Gnu | Gnutls | 3.2.9 | All | All | All |
| Application | Gnu | Gnutls | 3.1.0 | All | All | All |
| Application | Gnu | Gnutls | 3.1.1 | All | All | All |
| Application | Gnu | Gnutls | 3.1.10 | All | All | All |
| Application | Gnu | Gnutls | 3.1.11 | All | All | All |
| Application | Gnu | Gnutls | 3.1.12 | All | All | All |
| Application | Gnu | Gnutls | 3.1.13 | All | All | All |
| Application | Gnu | Gnutls | 3.1.14 | All | All | All |
| Application | Gnu | Gnutls | 3.1.15 | All | All | All |
| Application | Gnu | Gnutls | 3.1.16 | All | All | All |
| Application | Gnu | Gnutls | 3.1.17 | All | All | All |
| Application | Gnu | Gnutls | 3.1.18 | All | All | All |
| Application | Gnu | Gnutls | 3.1.19 | All | All | All |
| Application | Gnu | Gnutls | 3.1.2 | All | All | All |
| Application | Gnu | Gnutls | 3.1.3 | All | All | All |
| Application | Gnu | Gnutls | 3.1.4 | All | All | All |
| Application | Gnu | Gnutls | 3.1.5 | All | All | All |
| Application | Gnu | Gnutls | 3.1.6 | All | All | All |
| Application | Gnu | Gnutls | 3.1.7 | All | All | All |
| Application | Gnu | Gnutls | 3.1.8 | All | All | All |
| Application | Gnu | Gnutls | 3.1.9 | All | All | All |
| Application | Gnu | Gnutls | 3.2.0 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Gnu | Gnutls | 3.2.1 | All | All | All |
| Application | Gnu | Gnutls | 3.2.2 | All | All | All |
| Application | Gnu | Gnutls | 3.2.3 | All | All | All |
| Application | Gnu | Gnutls | 3.2.4 | All | All | All |
| Application | Gnu | Gnutls | 3.2.5 | All | All | All |
| Application | Gnu | Gnutls | 3.2.6 | All | All | All |
| Application | Gnu | Gnutls | 3.2.7 | All | All | All |
| Application | Gnu | Gnutls | 3.2.8 | All | All | All |
| Application | Gnu | Gnutls | 3.2.8.1 | All | All | All |
| Application | Gnu | Gnutls | 3.2.9 | All | All | All |
| Application | Gnu | Gnutls | All | All | All | All |
| Application | Gnu | Gnutls | All | All | All | All |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|
| oss-sec: Re: CVE Request - GnuTLS corrects flaw in certificate verification (3.1.x/3.2.x) | MLIST | seclists.org | |
| USN-2121-1: GnuTLS vulnerability \| Ubuntu | UBUNTU | www.ubuntu.com | |
| Fix bug that prevented the rejection of v1 intermediate CA certificates. - Gitorious | CONFIRM | www.gitorious.org | Exploit, Patc |
| oss-sec: CVE Request - GnuTLS corrects flaw in certificate verification (3.1.x/3.2.x) | MLIST | seclists.org | |
| GnuTLS | CONFIRM | www.gnutls.org | Vendor Advi |
| Debian -- Security Information -- DSA-2866-1 gnutls26 | DEBIAN | www.debian.org | |
| GnuTLS CVE-2014-1959 Certificate Validation Security Bypass Weakness | BID | www.securityfocus.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, a |

No vendor comments have been submitted for this CVE.

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

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