# CVE-2018-10844

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2018-10844 |
| **State** | PUBLIC |
| **Assigner** | secalert@redhat.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2018-08-22 13:29:00 UTC |
| **Updated** | 2023-02-13 04:50:00 UTC |
| **Description** | It was found that the GnuTLS implementation of HMAC-SHA-256 was vulnerable to a Lucky thirteen style attack. Remote a |

## Risk And Classification

**Problem Types:** CWE-385

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Canonical | Ubuntu Linux | 16.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.10 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 19.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 16.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.10 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 19.04 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Operating System | Fedoraproject | Fedora | 31 | All | All | All |
| Operating System | Fedoraproject | Fedora | 32 | All | All | All |
| Operating System | Fedoraproject | Fedora | 31 | All | All | All |
| Operating System | Fedoraproject | Fedora | 32 | All | All | All |
| Application | Gnu | Gnutls | All | All | All | All |
| Application | Gnu | Gnutls | 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 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 |
|---|
| [SECURITY] Fedora 31 Update: mingw-gnutls-3.6.13-1.fc31 - package-announce - Fedora Mailing-Lists |
| [SECURITY] [DLA 1560-1] gnutls28 security update |
| Red Hat Customer Portal |
| CVE-2018-10844 - Red Hat Customer Portal |
| [SECURITY] Fedora 32 Update: mingw-gnutls-3.6.13-1.fc32 - package-announce - Fedora Mailing-Lists |
| Malformed Request |
| Red Hat Customer Portal |
| [SECURITY] Fedora 31 Update: mingw-gnutls-3.6.13-1.fc31 - package-announce - Fedora Mailing-Lists |
| 1582571 – (CVE-2018-10844) CVE-2018-10844 gnutls: HMAC-SHA-256 vulnerable to Lucky thirteen attack due to not enough dummy functic |
| 1582571 – (CVE-2018-10844) CVE-2018-10844 gnutls: HMAC-SHA-256 vulnerable to Lucky thirteen attack due to not enough dummy functic |
| USN-3999-1: GnuTLS vulnerabilities \| Ubuntu security notices |
| Address issues in record layer decoding (!657) · Merge Requests · gnutls / GnuTLS · GitLab |
| [SECURITY] Fedora 32 Update: mingw-gnutls-3.6.13-1.fc32 - package-announce - Fedora Mailing-Lists |
| eprint.iacr.org/2018/747 |
| CVE Program record |
| NVD vulnerability detail |

No vendor comments have been submitted for this CVE.

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