



# CVE-2018-10844

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2018-10844
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-08-22 13:29:00 UTC
<b>Updated</b>	2023-02-13 04:50:00 UTC
<b>Description</b>	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	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.04	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Gnutls</a>	All	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Gnutls</a>	All	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All

Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	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 function

1582571 – (CVE-2018-10844) CVE-2018-10844 gnutls: HMAC-SHA-256 vulnerable to Lucky thirteen attack due to not enough dummy function

USN-3999-1: GnuTLS vulnerabilities | Ubuntu security notices

Address issues in record layer decoding (I657) · 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.

© 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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**