CVE-2018-10845

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-10845
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-384 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	S
[SECURITY] Fedora 31 Update: mingw-gnutls-3.6.13-1.fc31 - package-announce - Fedora Mailing-Lists	M
[SECURITY] [DLA 1560-1] gnutls28 security update	M
Red Hat Customer Portal	F
[SECURITY] Fedora 32 Update: mingw-gnutls-3.6.13-1.fc32 - package-announce - Fedora Mailing-Lists	M
Malformed Request	E
Red Hat Customer Portal	F
[SECURITY] Fedora 31 Update: mingw-gnutls-3.6.13-1.fc31 - package-announce - Fedora Mailing-Lists	F
1582572 – (CVE-2018-10845) CVE-2018-10845 gnutls: HMAC-SHA-384 vulnerable to Lucky thirteen attack due to use of wrong constant	C
USN-3999-1: GnuTLS vulnerabilities | Ubuntu security notices	U
1582572 – (CVE-2018-10845) CVE-2018-10845 gnutls: HMAC-SHA-384 vulnerable to Lucky thirteen attack due to use of wrong constant	M
CVE-2018-10845 - Red Hat Customer Portal	M
Address issues in record layer decoding (!657) · Merge Requests · gnutls / GnuTLS · GitLab	C
[SECURITY] Fedora 32 Update: mingw-gnutls-3.6.13-1.fc32 - package-announce - Fedora Mailing-Lists	F
eprint.iacr.org/2018/747	M
CVE Program record	C
NVD vulnerability detail	N

No vendor comments have been submitted for this CVE.

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