CVE-2015-8036

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-8036
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-11-02 19:59:00 UTC
Updated	2019-06-19 13:59:00 UTC
Description	Heap-based buffer overflow in ARM mbed TLS (formerly PolarSSL) 1.3.x before 1.3.14 and 2.x before 2.1.2 allows remote

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Arm	Mbed Tls	All	All	All	All
Application	Arm	Mbed Tls	All	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Application	Polarssl	Polarssl	All	All	All	All

References

Reference	Source	Link	T
guidovranken.files.wordpress.com/2015/10/cve-2015-5291.pdf	MISC	guidovranken.files.wordpress.com	T
mbed TLS Security Advisory 2015-01 - Tech Updates	CONFIRM	tls.mbed.org	V
[SECURITY] Fedora 21 Update: mbedtls-1.3.14-1.fc21	FEDORA	lists.fedoraproject.org	M

CVE-2015-5291: remote heap corruption in ARM mbed TLS / PolarSSL | Guido Vranken	MISC	guidovranken.wordpress.com	T
openSUSE-SU-2016:1928-1: moderate: Security update for polarssl	SUSE	lists.opensuse.org	M
Debian -- Security Information -- DSA-3468-1 polarssl	DEBIAN	www.debian.org	M
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

No vendor comments have been submitted for this CVE.

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