CVE-2015-5291

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-5291
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-11-02 19:59:00 UTC
Updated	2019-06-19 13:38:00 UTC
Description	Heap-based buffer overflow in PolarSSL 1.x before 1.2.17 and ARM mbed TLS (formerly PolarSSL) 1.3.x before 1.3.14 and

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	22	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.1	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

Application	Polarssl	Polarssl	All	All	All	All

References

Reference	Source	Link
[security-announce] openSUSE-SU-2015:2257-1: important: Security update	SUSE	lists.opensuse.org
[SECURITY] Fedora 22 Update: mbedtls-1.3.14-1.fc22	FEDORA	lists.fedoraproject.org
guidovranken.files.wordpress.com/2015/10/cve-2015-5291.pdf	MISC	guidovranken.files.wordpress.com
[SECURITY] Fedora 23 Update: mbedtls-2.1.2-1.fc23	FEDORA	lists.fedoraproject.org
mbed TLS: Multiple vulnerabilities (GLSA 201706-18) — Gentoo Security	GENTOO	security.gentoo.org
mbed TLS Security Advisory 2015-01 - Tech Updates	CONFIRM	tls.mbed.org
[SECURITY] Fedora 21 Update: mbedtls-1.3.14-1.fc21	FEDORA	lists.fedoraproject.org
CVE-2015-5291: remote heap corruption in ARM mbed TLS / PolarSSL | Guido Vranken	MISC	guidovranken.wordpress.com
openSUSE-SU-2015:2371-1: moderate: Security update for polarssl	SUSE	lists.opensuse.org
Debian -- Security Information -- DSA-3468-1 polarssl	DEBIAN	www.debian.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

710439 Gentoo Linux mbed Transport Layer Security (TLS) Multiple Vulnerabilities (GLSA 201706-18)