CVE-2018-9988

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-9988
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-04-10 19:29:00 UTC
Updated	2021-11-30 21:43:00 UTC
Description	ARM mbed TLS before 2.1.11, before 2.7.2, and before 2.8.0 has a buffer over-read in ssl_parse_server_key_exchange() t

Risk And Classification

Problem Types: CWE-125

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	2.8.0	rc1	All	All
Application	Arm	Mbed Tls	All	All	All	All
Application	Arm	Mbed Tls	2.8.0	rc1	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All

References

Reference	Source	Link	Tags
Prevent arithmetic overflow on bounds check · ARMmbed/mbedtls@027f84c · GitHub	CONFIRM	github.com	Patch, Third P
Mbed TLS 2.8.0, 2.7.2 and 2.1.11 released - Tech Updates - mbed TLS (Previously PolarSSL)	CONFIRM	tls.mbed.org	Release Note
Add bounds check before signature length read · ARMmbed/mbedtls@a1098f8 · GitHub	CONFIRM	github.com	Patch, Third P
[SECURITY] [DLA 2826-1] mbedtls security update	MLIST	lists.debian.org	
[SECURITY] [DLA 1518-1] polarssl security update	MLIST	lists.debian.org	Mailing List, T
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, an

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

178909 Debian Security Update for mbedtls (DLA 2826-1)