CVE-2020-36478

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-36478
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-23 02:15:00 UTC
Updated	2023-01-11 17:01:00 UTC
Description	An issue was discovered in Mbed TLS before 2.25.0 (and before 2.16.9 LTS and before 2.7.18 LTS). A NULL algorithm par

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Arm	Mbed Tls	All	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Hardware	Siemens	Logo! Cmr2020	-	All	All	All
Operating System	Siemens	Logo! Cmr2020 Firmware	All	All	All	All
Hardware	Siemens	Logo! Cmr2040	-	All	All	All
Operating System	Siemens	Logo! Cmr2040 Firmware	All	All	All	All
Hardware	Siemens	Simatic Rtu3000c	-	All	All	All
Operating System	Siemens	Simatic Rtu3000c Firmware	All	All	All	All
Hardware	Siemens	Simatic Rtu3030c	-	All	All	All
Operating System	Siemens	Simatic Rtu3030c Firmware	All	All	All	All
Hardware	Siemens	Simatic Rtu3031c	-	All	All	All
Operating System	Siemens	Simatic Rtu3031c Firmware	All	All	All	All
Hardware	Siemens	Simatic Rtu3041c	-	All	All	All
Operating System	Siemens	Simatic Rtu3041c Firmware	All	All	All	All

References

Reference	Source	Link
cert-portal.siemens.com/productcert/pdf/ssa-756638.pdf	CONFIRM	cert-portal.s
Release Mbed TLS 2.7.18 · ARMmbed/mbedtls · GitHub	MISC	github.com
[SECURITY] [DLA 3249-1] mbedtls security update	MLIST	lists.debian.
Release Mbed TLS 2.16.9 · ARMmbed/mbedtls · GitHub	MISC	github.com
[SECURITY] [DLA 2826-1] mbedtls security update	MLIST	lists.debian.
Certificate verification discrepancy between OpenSSL and mbed TLS · Issue #3629 · ARMmbed/mbedtls · GitHub	MISC	github.com
Release Mbed TLS 2.25.0 · ARMmbed/mbedtls · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.or
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 178909 Debian Security Update for mbedtls (DLA 2826-1)
- 181446 Debian Security Update for mbedtls (DLA 3249-1)
- 590717 Siemens LOGO! CMR and SIMATIC RTU 3000 Multiple Vulnerabilities (ICSA-21-257-20)
- 591119 Siemens LOGO! CMR Family and SIMATIC RTU 3000 Family Multiple Vulnerabilities (ssa-756638)
- 710702 Gentoo Linux Mbed Transport Layer Security (TLS) Multiple Vulnerabilities (GLSA 202301-08)