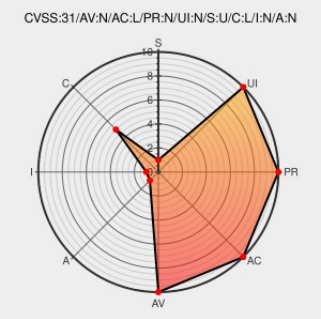
CVE-2018-19440

Published on: 01/29/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:39 PM UTC

CVE-2018-19440

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Trusted Firmware-a from Arm contain the following vulnerability:

ARM Trusted Firmware-A allows information disclosure.

CVE-2018-19440 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.3 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	NONE	NONE

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
BL31: Use helper function to save registers in SMC handler by soby-mathew · Pull Request #1710 · ARM-software/arm-trusted-firmware · GitHub	Patch, Third Party Advisory, github.com, text/html	CONFIRM github.com/ARM-software/arm-trusted-firmware/pull/1710

Trusted Firmware A Security Advisory TFV 8 · ARM-software/arm-trusted-firmware Wiki · GitHub	Exploit Third Party Advisory github.com text/html	CONFIRM github.com/ARM-software/arm-trusted-firmware/wiki/Trusted-Firmware-A-Security-Advisory-TFV-8

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Arm	Trusted Firmware-a	All	All	All	All

cpe:2.3:a:arm:trusted_firmware-a:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→