



CVE-2021-40327

Published on: 01/13/2022 12:00:00 AM UTC

Last Modified on: 01/25/2022 02:35:00 PM UTC

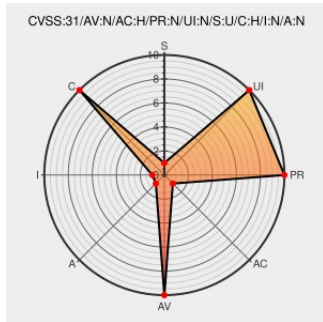
CVE-2021-40327

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Trusted Firmware-m](#) from [Trustedfirmware](#) contain the following vulnerability:

Trusted Firmware-M (TF-M) 1.4.0, when Profile Small is used, has incorrect access control. NSPE can access a secure key (held by the Crypto service) based solely on knowledge of its key ID. For example, there is no authorization check associated with the relationship between a caller and a key owner.

CVE-2021-40327 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.9 - MEDIUM**

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

CVSS2 Score: **2.6 - LOW**

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Arm Security Center	developer.arm.com text/html	arm MISC developer.arm.com/support/arm-security-updates
Advisory	tf-m-user-guide.trustedfirmware.org	CONFIRM tf-m-user-

TFMV-4 — [text/html](#) [guide.trustedfirmware.org/docs/security/security_advisories/profile_small_key_id_encodin](#)
Trusted
Firmware-M
v1.5.0+
(f07cc31)
documentation

trusted- [git.trustedfirmware.org](#) [MISC git.trustedfirmware.org/TF-M/trusted-firmware-m.git/](#)
firmware-m.git [text/html](#)
- Trusted
Firmware for
M profile Arm
CPUs

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Trustedfirmware	Trusted Firmware-m	1.4.0	All	All	All

cpe:2.3:a:trustedfirmware:trusted_firmware-m:1.4.0:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-40327 : Trusted Firmware-M TF-M 1.4.0, when Profile Small is used, has incorrect access control. NSPE ca... twitter.com/i/web/status/1...	2022-01-13 16:06:02
/r/netcve	CVE-2021-40327	2022-01-13 17:39:03

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)