

CVE-2021-27562

Arm Trusted Firmware Out-of-Bounds Write Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

In Arm Trusted Firmware M through 1.2, the NS world may trigger a system halt, an overwrite of secure data, or the printing out of secure data when calling secure functions under the NSPE handler mode.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 5.5 Medium · NVD	EPSS 0.031 87.5th percentile · FIRST	CISA DEADLINE Nov 17, 2021 KEV since 2021 · listed over a year
---	--	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.031 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 5.5	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
trusted firmware-m	≤ 1.2.0	after 1.2.0	NVD

Sources

Vendor guidance	developer.arm.com/support/arm-security-updates	NVD	nvd.nist.gov/vuln/detail/CVE-2021-27562
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2021-14313
Current data	evulnable.com/vulnerability-management/cve/CVE-2021-27562		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.