



CVE-2020-6174

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2020-6174
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-05 16:15:00 UTC
Updated	2020-02-07 19:19:00 UTC
Description	TUF (aka The Update Framework) through 0.12.1 has Improper Verification of a Cryptographic Signature.

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Linuxfoundation	The Update Framework	All	All	All	All

References

Reference	Source	Link	Tags
Fix signature threshold by lukpueh · Pull Request #974 · theupdateframework/tuf · GitHub	CONFIRM	github.com	Patch, Third Party A
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[980723](#) Python (pip) Security Update for tuf (GHSA-pwqf-9h7j-7mv8)

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report