



CVE-2020-15163

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

Summary

CVE	CVE-2020-15163
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-09 18:15:00 UTC
Updated	2021-11-18 17:45:00 UTC
Description	Python TUF (The Update Framework) reference implementation before version 0.12 it will incorrectly trust a previously dow

Risk And Classification

Problem Types: CWE-345

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source
tuf · PyPI	MISC
Do not immediately verify latest root when rotating by trishankatdatadog · Pull Request #885 · theupdateframework/tuf · GitHub	MISC
Merge pull request #885 from trishankatdatadog:trishankatdatadog/corr... · theupdateframework/tuf@3d342e6 · GitHub	CONFIRM
Invalid root may become trusted root · Advisory · theupdateframework/tuf · GitHub	CONFIRM
Release tuf v0.12.0 · theupdateframework/tuf · GitHub	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[980046](#) Python (pip) Security Update for tuf (GHSA-f8mr-jv2c-v8mg)

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

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