CVE-2020-27743

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-27743
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-26 22:15:00 UTC
Updated	2020-11-02 16:37:00 UTC
Description	libtac in pam_tacplus through 1.5.1 lacks a check for a failure of RAND_bytes()/RAND_pseudo_bytes(). This could lead to u

Risk And Classification

Problem Types: CWE-330

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pam Tacplus Project	Pam Tacplus	All	All	All	All

References

Reference	Source	Link
RFC 8907 - The Terminal Access Controller Access-Control System Plus (TACACS+) Protocol	MISC	tools.ietf
Check for failure of OpenSSL RAND_[pseudo_]bytes by deastoe · Pull Request #163 · kravietz/pam_tacplus · GitHub	MISC	github.co
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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