CVE-2021-3505

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2021-3505
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-19 21:15:00 UTC
Updated	2023-11-07 03:38:00 UTC
Description	A flaw was found in libtpms in versions before 0.8.0. The TPM 2 implementation returns 2048 bit keys with ~1984 bit streng

Risk And Classification

Problem Types: CWE-331

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Libtpms Project	Libtpms	All	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

References

Reference	Source	Link
1950046 – (CVE-2021-3505) CVE-2021-3505 libtpms: RSA keys weaker than expected	MISC	bugz
[SECURITY] Fedora 33 Update: libtpms-0.8.2-0.20210426git729fc6a4ca.fc33 - package-announce - Fedora Mailing-Lists		lists.f
[SECURITY] Fedora 33 Update: libtpms-0.8.2-0.20210426git729fc6a4ca.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.f
[libtpms 0.7] TPM2_CreatePrimary creates prime numbers with 32 zero bits · Issue #183 · stefanberger/libtpms · GitHub	MISC	githu
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.r

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

184150 Debian Security Update for libtpms (CVE-2021-3505)

281253 Fedora Security Update for libtpms (FEDORA-2021-cfdc434610)

Free CVE JSON API cve.report/api

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