



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.
[SECURITY] Fedora 33 Update: libtpms-0.8.2-0.20210426git729fc6a4ca.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.
[libtpms 0.7] TPM2_CreatePrimary creates prime numbers with 32 zero bits · Issue #183 · stefanberger/libtpms · GitHub	MISC	github
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)

© [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](#)