



CVE-2021-3623

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

Summary

CVE	CVE-2021-3623
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-02 23:15:00 UTC
Updated	2023-11-07 03:38:00 UTC
Description	A flaw was found in libtpms. The flaw can be triggered by specially-crafted TPM 2 command packets containing illegal values.

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	34	All	All	All
Application	Libtpms Project	Libtpms	All	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

References

Reference
[SECURITY] Fedora 34 Update: libtpms-0.8.4-1.20210624gita594c4692a.fc34.1 - package-announce - Fedora Mailing-Lists
tpm2: Add maxSize parameter to TPM2B_Marshal for sanity checks · stefanberger/libtpms@7981d9a · GitHub
1976806 – (CVE-2021-3623) CVE-2021-3623 libtpms: out-of-bounds access when trying to resume the state of the vTPM
tpm2: Restore original value if unmarsalled value was illegal · stefanberger/libtpms@2e6173c · GitHub
Reset buffer size indicators that are too large and check for maximum size on marshalling by stefanberger · Pull Request #223 · stefanberger/libtpms
tpm2: Reset TPM2B buffer sizes after test fails for valid buffer size · stefanberger/libtpms@2f30d62 · GitHub
[SECURITY] Fedora 34 Update: libtpms-0.8.4-1.20210624gita594c4692a.fc34.1 - package-announce - Fedora Mailing-Lists
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159724](#) Oracle Enterprise Linux Security Update for libtpms (ELSA-2022-9240)

[182922](#) Debian Security Update for libtpms (CVE-2021-3623)

[281671](#) Fedora Security Update for libtpms (FEDORA-2021-465b5c3b67)

[752991](#) SUSE Enterprise Linux Security Update for libtpms (SUSE-SU-2022:4457-1)

© [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](#)