



CVE-2019-17362

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2019-17362
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-10-09 01:15:00 UTC
Updated	2023-12-14 03:15:00 UTC
Description	In LibTomCrypt through 1.18.2, the der_decode_utf8_string function (in der_decode_utf8_string.c) does not properly detect

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Libtom	Libtomcrypt	All	All	All	All

References

Reference	Source	Link
[SECURITY] [DLA 1951-1] libtomcrypt security update	MLIST	lists.debian.org
Fixes #507 by werew · Pull Request #508 · libtom/libtomcrypt · GitHub	MISC	github.com
[SECURITY] Fedora 38 Update: perl-CryptX-0.080-1.fc38 - package-announce - Fedora Mailing-Lists		lists.fedoraproje
[security-announce] openSUSE-SU-2019:2514-1: moderate: Security update f	SUSE	lists.opensuse.o
[SECURITY] Fedora 39 Update: perl-CryptX-0.080-1.fc39 - package-announce - Fedora Mailing-Lists		lists.fedoraproje
[security-announce] openSUSE-SU-2019:2454-1: moderate: Security update f	SUSE	lists.opensuse.o
CVE-2019-17362 LibTomCrypt UTF-8 der_decode_utf8_string.c der_decode_utf8_string out-of-bounds read	MISC	vuldb.com
CVE-2019-17362 - vulnerability in der_decode_utf8_string · Issue #507 · libtom/libtomcrypt · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

284809 Fedora Security Update for perl (FEDORA-2023-b4b9b38f23)
285113 Fedora Security Update for perl (FEDORA-2023-1f0ac1260e)
503366 Alpine Linux Security Update for perl-cryptx
505914 Alpine Linux Security Update for perl-cryptx
670489 EulerOS Security Update for libtomcrypt (EulerOS-SA-2021-2247)
670515 EulerOS Security Update for libtomcrypt (EulerOS-SA-2021-2273)
670545 EulerOS Security Update for libtomcrypt (EulerOS-SA-2021-2303)
901228 Common Base Linux Mariner (CBL-Mariner) Security Update for libtomcrypt (7275)
904632 Common Base Linux Mariner (CBL-Mariner) Security Update for libtomcrypt (7275-1)

© [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](#).

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