



CVE-2023-36328

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

Summary

CVE	CVE-2023-36328
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-01 16:15:00 UTC
Updated	2023-11-07 04:16:00 UTC
Description	Integer Overflow vulnerability in mp_grow in libtom libtommath before commit beba892bc0d4e4ded4d667ab1d2a94f4d7510

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	38	All	All	All
Application	Libtom	Libtommath	All	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 37 Update: libtommath-1.2.0-11.fc37 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Fix possible integer overflow by czurnieden · Pull Request #546 · libtom/libtommath · GitHub	MISC	github.com
[SECURITY] Fedora 39 Update: libtommath-1.2.0-13.fc39 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 37 Update: libtommath-1.2.0-11.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 39 Update: libtommath-1.2.0-13.fc39 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 38 Update: libtommath-1.2.0-12.fc38 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 38 Update: libtommath-1.2.0-12.fc38 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
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

199792	Ubuntu Security Notification for LibTomMath Vulnerability (USN-6402-1)
199953	Ubuntu Security Notification for LibTomMath Vulnerability (USN-6402-2)
284525	Fedora Security Update for libtommath (FEDORA-2023-f5680e3b4b)
285271	Fedora Security Update for libtommath (FEDORA-2023-f357a25877)
356242	Amazon Linux Security Advisory for libtommath : ALASANSIBLE2-2023-010
356379	Amazon Linux Security Advisory for libtommath : ALAS2023-2023-370
356465	Amazon Linux Security Advisory for libtommath : ALAS2ANSIBLE2-2023-010
673326	EulerOS Security Update for libtommath (EulerOS-SA-2024-1278)
673355	EulerOS Security Update for libtommath (EulerOS-SA-2023-3014)
673409	EulerOS Security Update for libtommath (EulerOS-SA-2023-3185)
673467	EulerOS Security Update for libtommath (EulerOS-SA-2023-3037)
673468	EulerOS Security Update for libtommath (EulerOS-SA-2023-3340)
673761	EulerOS Security Update for libtommath (EulerOS-SA-2023-3220)
673978	EulerOS Security Update for libtommath (EulerOS-SA-2023-3308)
907298	Common Base Linux Mariner (CBL-Mariner) Security Update for libtommath (28639-1)
907336	Common Base Linux Mariner (CBL-Mariner) Security Update for tcl (28627-1)

© [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](#)