



CVE-2022-40320

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

Summary

CVE	CVE-2022-40320
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-09 21:15:00 UTC
Updated	2023-11-07 03:52:00 UTC
Description	cfg_tilde_expand in confuse.c in libConfuse 3.3 has a heap-based buffer over-read.

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Operating System	Fedoraproject	Fedora	37	All	All	All
Application	Libconfuse Project	Libconfuse	3.3	All	All	All

References

Reference	Source	Link	Tag
[SECURITY] Fedora 37 Update: libconfuse-3.3-7.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
[BUG] heap buffer overflow in cfg_tilde_expand · Issue #163 · libconfuse/libconfuse · GitHub	MISC	github.com	
[SECURITY] Fedora 35 Update: libconfuse-3.3-7.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
[SECURITY] Fedora 37 Update: libconfuse-3.3-7.fc37 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 36 Update: libconfuse-3.3-7.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
[SECURITY] Fedora 35 Update: libconfuse-3.3-7.fc35 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 36 Update: libconfuse-3.3-7.fc36 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

181363 Debian Security Update for libconfuse (CVE-2022-40320)
283132 Fedora Security Update for libconfuse (FEDORA-2022-9b67d67195)
283133 Fedora Security Update for libconfuse (FEDORA-2022-de992c68d0)
354749 Amazon Linux Security Advisory for libconfuse : ALAS-2023-1692
753380 SUSE Enterprise Linux Security Update for libconfuse0 (SUSE-SU-2022:3807-1)
903903 Common Base Linux Mariner (CBL-Mariner) Security Update for libconfuse (10956)
903923 Common Base Linux Mariner (CBL-Mariner) Security Update for libconfuse (10925)
904775 Common Base Linux Mariner (CBL-Mariner) Security Update for libconfuse (10925-1)
905668 Common Base Linux Mariner (CBL-Mariner) Security Update for libconfuse (10956-1)
906571 Common Base Linux Mariner (CBL-Mariner) Security Update for libconfuse (10956-3)

© [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](#)