



CVE-2021-45926

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

Summary

CVE	CVE-2021-45926
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-01 01:15:00 UTC
Updated	2022-12-09 16:39:00 UTC
Description	MDB Tools (aka mdbtools) 0.9.2 has a stack-based buffer overflow (at 0x7ffd0c689be0) in mdb_numeric_to_string (called f

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mdbtools Project	Mdbtools	0.9.2	All	All	All

References

Reference	Source	Link	Tags
35972 - oss-fuzz - OSS-Fuzz: Fuzzing the planet - Monorail	MISC	bugs.chromium.org	
Version 0.9.3, final · mdbtools/mdbtools@373b7ff · GitHub	MISC	github.com	
mdbtools: Multiple Vulnerabilities (GLSA 202208-12) — Gentoo security	GENTOO	security.gentoo.org	
oss-fuzz-vulns/OSV-2021-958.yaml at main · google/oss-fuzz-vulns · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[710588](#) Gentoo Linux mdbtools Multiple Vulnerabilities (GLSA 202208-12)

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