



CVE-2022-20803

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

Summary

CVE	CVE-2022-20803
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-17 18:15:00 UTC
Updated	2023-10-01 11:15:00 UTC
Description	A vulnerability in the OLE2 file parser of Clam AntiVirus (ClamAV) versions 0.104.0 through 0.104.2 could allow an unauth

Risk And Classification

Problem Types: CWE-415

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Clamav	Clamav	All	All	All	All

References

Reference	Source	Link	Tags
ClamAV® blog: ClamAV 0.105.0, 0.104.3, 0.103.6 released	CISCO	blog.clamav.net	
ClamAV: Multiple Vulnerabilities (GLSA 202310-01) — Gentoo security	GENTOO	security.gentoo.org	
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

[690872](#) Free Berkeley Software Distribution (FreeBSD) Security Update for clamav (b2407db1-d79f-11ec-a15f-589cfc0f81b0)

[710761](#) Gentoo Linux ClamAV Multiple Vulnerabilities (GLSA 202310-01)

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](#)