



# CVE-2022-20792

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2022-20792   |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | psirt@cisco.com  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2022-08-10 09:15:00 UTC  |
| <b>Updated</b>         | 2023-10-01 11:15:00 UTC  |
| <b>Description</b>     | A vulnerability in the regex module used by the signature database load module of Clam AntiVirus (ClamAV) versions 0.104 |

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                 | Product                | Version | Update | Edition | Language |
|-------------|------------------------|------------------------|---------|--------|---------|----------|
| Application | <a href="#">Clamav</a> | <a href="#">Clamav</a> | All     | All    | All     | All      |
| Application | <a href="#">Clamav</a> | <a href="#">Clamav</a> | All     | All    | All     | All      |

## References

| Reference   | Source  | Link   | Tags                |
|---|---------|--|---------------------|
| ClamAV@ blog: ClamAV 0.105.0, 0.104.3, 0.103.6 released             | CISCO   | <a href="http://blog.clamav.net">blog.clamav.net</a>         |                     |
| ClamAV: Multiple Vulnerabilities (GLSA 202310-01) — Gentoo security | GENTOO  | <a href="http://security.gentoo.org">security.gentoo.org</a> |                     |
| CVE Program record  | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>                 | canonical           |
| NVD vulnerability detail  | NVD     | <a href="http://nvd.nist.gov">nvd.nist.gov</a>               | canonical, analysis |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

- [179350](#) Debian Security Update for clamav (DLA 3042-1)
- [180857](#) Debian Security Update for clamav (CVE-2022-20792)
- [198788](#) Ubuntu Security Notification for ClamAV Vulnerabilities (USN-5423-1)
- [500101](#) Alpine Linux Security Update for clamav

|        |   |
|--------|---|
| 690872 | Free Berkeley Software Distribution (FreeBSD) Security Update for clamav (b2407db1-d79f-11ec-a15f-589cfc0f81b0) |
| 710761 | Gentoo Linux ClamAV Multiple Vulnerabilities (GLSA 202310-01)   |
| 752118 | SUSE Enterprise Linux Security Update for clamav (SUSE-SU-2022:1644-1)  |
| 752121 | SUSE Enterprise Linux Security Update for clamav (SUSE-SU-2022:1647-1)  |

© [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](#)**