



CVE-2019-15961

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

Summary

CVE	CVE-2019-15961
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-15 19:15:00 UTC
Updated	2022-10-19 18:54:00 UTC
Description	A vulnerability in the email parsing module Clam AntiVirus (ClamAV) Software versions 0.102.0, 0.101.4 and prior could allow

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Cisco	Email Security Appliance Firmware	11.1.1-042	All	All	All
Operating System	Cisco	Email Security Appliance Firmware	11.1.2-023	All	All	All
Operating System	Cisco	Email Security Appliance Firmware	11.1.1-042	All	All	All
Operating System	Cisco	Email Security Appliance Firmware	11.1.2-023	All	All	All
Application	Clamav	Clamav	0.102.0	All	All	All
Application	Clamav	Clamav	All	All	All	All
Application	Clamav	Clamav	0.102.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All

References

Reference	Source	L
[SECURITY] [DLA 2108-1] clamav security update	MLIST	li
ClamAV: Multiple vulnerabilities (GLSA 202003-46) — Gentoo security	GENTOO	s
Cisco Bug: CSCvr56010 - Opened to track: ClamAV for Cisco Email Security Appliance (ESA) Denial of Service Vulnerability	CISCO	c
USN-4230-2: ClamAV vulnerability Ubuntu security notices Ubuntu	UBUNTU	u

Bug 12380 – MIME Denial of Service Vulnerability	CISCO	t
CVE Program record	CVE.ORG	v
NVD vulnerability detail	NVD	r

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 500096 Alpine Linux Security Update for clamav
- 503821 Alpine Linux Security Update for clamav
- 750483 OpenSUSE Security Update for clamav (openSUSE-SU-2020:2276-1)
- 750485 OpenSUSE Security Update for clamav (openSUSE-SU-2020:2268-1)
- 900004 CBL-Mariner Linux Security Update for clamav 0.101.2
- 903412 Common Base Linux Mariner (CBL-Mariner) Security Update for clamav (3169)

© [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](#)