



CVE-2020-3350

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

Summary

CVE	CVE-2020-3350
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-18 03:15:00 UTC
Updated	2023-11-07 03:22:00 UTC
Description	A vulnerability in the endpoint software of Cisco AMP for Endpoints and Clam AntiVirus could allow an authenticated, local :

Risk And Classification

Problem Types: CWE-362

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	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Application	Cisco	Advanced Malware Protection For Endpoints	All	All	All	All
Application	Cisco	Advanced Malware Protection For Endpoints	All	All	All	All
Application	Cisco	Advanced Malware Protection For Endpoints	All	All	All	All
Application	Cisco	Advanced Malware Protection For Endpoints	All	All	All	All
Application	Cisco	Clam Antivirus	All	All	All	All
Application	Cisco	Clam Antivirus	All	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All

References

Reference	Source	Link	Ta
-----------	--------	------	----

[SECURITY] Fedora 31 Update: clamav-0.102.4-1.fc31 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 32 Update: clamav-0.102.4-1.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
USN-4435-2: ClamAV vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	
Cisco AMP for Endpoints and ClamAV Privilege Escalation Vulnerability	CISCO	tools.cisco.com	Ve
USN-4435-1: ClamAV vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	
[SECURITY] Fedora 31 Update: clamav-0.102.4-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
ClamAV: Multiple vulnerabilities (GLSA 202007-23) — Gentoo security	GENTOO	security.gentoo.org	
[SECURITY] Fedora 32 Update: clamav-0.102.4-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
[SECURITY] [DLA 2314-1] clamav security update	MLIST	lists.debian.org	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[500099](#) Alpine Linux Security Update for clamav

[503824](#) Alpine Linux Security Update for clamav

[690450](#) Free Berkeley Software Distribution (FreeBSD) Security Update for clamav (f7a02651-c798-11ea-81d6-6805cabe6ebb)

[750483](#) OpenSUSE Security Update for clamav (openSUSE-SU-2020:2276-1)

[750485](#) OpenSUSE Security Update for clamav (openSUSE-SU-2020:2268-1)

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report