



CVE-2018-0202

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

Summary

CVE	CVE-2018-0202
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-27 09:29:00 UTC
Updated	2019-03-26 16:02:00 UTC
Description	clamscan in ClamAV before 0.99.4 contains a vulnerability that could allow an unauthenticated, remote attacker to cause a

Risk And Classification

Problem Types: CWE-125

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	17.10	All	All	All
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	17.10	All	All	All
Application	Clamav	Clamav	All	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All

References

Reference	Source	Link	Tags
USN-3592-2: ClamAV vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com	Third Party Advisory
USN-3592-1: ClamAV vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	Third Party Advisory
Bug 11973 – Heap overflow pdf_parse_array pdfng.c:566	CONFIRM	bugzilla.clamav.net	Issue Tracking, Patch, Third Part

[SECURITY] [DLA 1307-1] clamav security update	MLIST	lists.debian.org	Mailing List, Third Party Advisory
Bug 11980 – Heap overflow in pdf_parse_string	CONFIRM	bugzilla.clamav.net	Issue Tracking, Third Party Advis
ClamAV: Multiple vulnerabilities (GLSA 201804-16) — Gentoo security	GENTOO	security.gentoo.org	Third Party Advisory
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

[500103](#) Alpine Linux Security Update for clamav

[503827](#) Alpine Linux Security Update for clamav

[710259](#) Gentoo Linux ClamAV Multiple Vulnerabilities (GLSA 201804-16)

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

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