



CVE-2017-12377

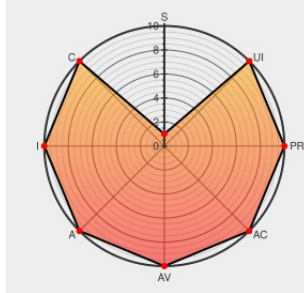
Published on: 01/26/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:30 PM UTC

CVE-2017-12377

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Clamav](#) from [Clamav](#) contain the following vulnerability:

ClamAV AntiVirus software versions 0.99.2 and prior contain a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or potentially execute arbitrary code on an affected device. The vulnerability is due to improper input validation checking mechanisms in mew packet files

sent to an affected device. A successful exploit could cause a heap-based buffer over-read condition in mew.c when ClamAV scans the malicious file, allowing the attacker to cause a DoS condition or potentially execute arbitrary code on the affected device.

CVE-2017-12377 has been assigned by [cisco](#) psirt@cisco.com to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **10 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
-------------	------	------

Bug 11943 – Heap overflow in zma_bswap_4861dc (mew.c)	Exploit Issue Tracking Vendor Advisory bugzilla.clamav.net text/html	CONFIRM bugzilla.clamav.net/show_bug.cgi?id=11943
[SECURITY] [DLA 1261-1] clamav security update	Mailing List Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20180128 [SECURITY] [DLA 1261-1] clamav security update
ClamAV® blog: ClamAV 0.99.3 has been released!	Release Notes Vendor Advisory blog.clamav.net text/html	CONFIRM blog.clamav.net/2018/01/clamav-0993-has-been-released.html
USN-3550-1: ClamAV vulnerabilities Ubuntu security notices Ubuntu	usn.ubuntu.com text/html	UBUNTU USN-3550-1
USN-3550-2: ClamAV vulnerabilities Ubuntu security notices	usn.ubuntu.com text/html	UBUNTU USN-3550-2
By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.		

Related QID Numbers

[500102](#) Alpine Linux Security Update for clamav

[710255](#) Gentoo Linux ClamAV Multiple Vulnerabilities (GLSA 201801-19)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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
cpe:2.3:a:clamav:clamav:*****:*						
cpe:2.3:o:debian:debian_linux:7.0:*****:*						
cpe:2.3:o:debian:debian_linux:7.0:*****:*						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)