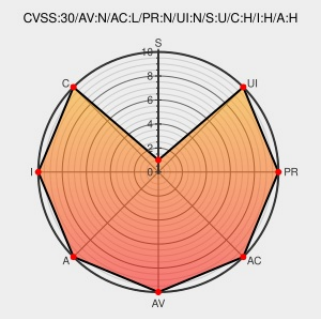
CVE-2017-12379

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

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

CVE-2017-12379

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



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 the message parsing function on an affected system. An unauthenticated, remote attacker could exploit this vulnerability by sending a crafted email to the affected device. This action could cause a messageAddArgument (in message.c) buffer overflow condition when ClamAV scans the malicious email, allowing the attacker to potentially cause a DoS condition or execute arbitrary code on an affected device.

CVE-2017-12379 has been assigned by 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 11944 – Heap overflow in messageAddArgument (message.c)	Exploit, Issue Tracking, Vendor Advisory, bugzilla.clamav.net, text/html	CONFIRM bugzilla.clamav.net/show_bug.cgi?id=11944
[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

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→

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