



# CVE-2017-12379

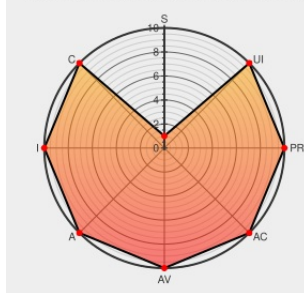
Published on: 01/26/2018 12:00:00 AM UTC

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

## CVE-2017-12379

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

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 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    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **10 - HIGH**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>COMPLETE</b>        | <b>COMPLETE</b>   | <b>COMPLETE</b>     |

## CVE References

| Description                                                           | Tags                                                                                                                                                             | Link                                                                                                                                                                                                                                  |
|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bug 11944 – Heap overflow in messageAddArgument (message.c)           | <a href="#">Exploit</a><br><a href="#">Issue Tracking</a><br><a href="#">Vendor Advisory</a><br><a href="#">bugzilla.clamav.net</a><br><a href="#">text/html</a> |  <a href="https://bugzilla.clamav.net/show_bug.cgi?id=11944">CONFIRM bugzilla.clamav.net/show_bug.cgi?id=11944</a>                                   |
| [SECURITY] [DLA 1261-1] clamav security update                        | <a href="#">Mailing List</a><br><a href="#">Third Party Advisory</a><br><a href="#">lists.debian.org</a><br><a href="#">text/html</a>                            |  <a href="#">MLIST [debian-lts-announce] 20180128 [SECURITY] [DLA 1261-1] clamav security update</a>                                                 |
| ClamAV® blog: ClamAV 0.99.3 has been released!                        | <a href="#">Release Notes</a><br><a href="#">Vendor Advisory</a><br><a href="#">blog.clamav.net</a><br><a href="#">text/html</a>                                 |  <a href="https://blog.clamav.net/2018/01/clamav-0993-has-been-released.html">CONFIRM blog.clamav.net/2018/01/clamav-0993-has-been-released.html</a> |
| USN-3550-1: ClamAV vulnerabilities   Ubuntu security notices   Ubuntu | <a href="#">usn.ubuntu.com</a><br><a href="#">text/html</a>                                                                                                      |  <a href="#">UBUNTU USN-3550-1</a>                                                                                                                   |
| USN-3550-2: ClamAV vulnerabilities   Ubuntu security notices          | <a href="#">usn.ubuntu.com</a><br><a href="#">text/html</a>                                                                                                      |  <a href="#">UBUNTU USN-3550-2</a>                                                                                                                   |

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](mailto: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                                                     | <a href="#">Clamav</a> | <a href="#">Clamav</a>       | All     | All    | All     | All      |
| Operating System                                                | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 7.0     | All    | All     | All      |
| Operating System                                                | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 7.0     | All    | All     | All      |
| <a href="#">cpe:2.3:a:clamav:clamav:*.***.***.***</a>           |                        |                              |         |        |         |          |
| <a href="#">cpe:2.3:o:debian:debian_linux:7.0:*.***.***.***</a> |                        |                              |         |        |         |          |
| <a href="#">cpe:2.3:o:debian:debian_linux:7.0:*.***.***.***</a> |                        |                              |         |        |         |          |

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#)