



# CVE-2018-0361

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

## Summary

<b>CVE</b>	CVE-2018-0361
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-07-16 17:29:00 UTC
<b>Updated</b>	2019-04-26 16:41:00 UTC
<b>Description</b>	ClamAV before 0.100.1 lacks a PDF object length check, resulting in an unreasonably long time to parse a relatively small f

## Risk And Classification

**Problem Types:** CWE-20

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Clamav</a>	<a href="#">Clamav</a>	All	All	All	All
Application	<a href="#">Clamav</a>	<a href="#">Clamav</a>	All	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All

## References

Reference	Source	Link	Tags
ClamAV: Multiple vulnerabilities (GLSA 201904-12) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	Third Pa
Clam AntiVirus File Processing Bugs Let Remote Users Deny Service - SecurityTracker	SECTRACK	<a href="http://www.securitytracker.com">www.securitytracker.com</a>	Third Pa
ClamAV@ blog: ClamAV 0.100.1 has been released!	CONFIRM	<a href="http://blog.clamav.net">blog.clamav.net</a>	Vendor /
[SECURITY] [DLA 1461-1] clamav security update	MLIST	<a href="http://lists.debian.org">lists.debian.org</a>	Mailing L
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonica
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonica

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

500092 Alpine Linux Security Update for clamav

503817 Alpine Linux Security Update for clamav

710172 Gentoo Linux ClamAV Multiple vulnerabilities (GLSA 201904-12)

© [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](#) 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](#)