



CVE-2017-6420

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

Summary

CVE	CVE-2017-6420
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-07 03:29:00 UTC
Updated	2018-10-21 10:29:00 UTC
Description	The wwunpack function in libclamav/wwunpack.c in ClamAV 0.99.2 allows remote attackers to cause a denial of service (use-after-free) via crafted PE files.

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Clamav	Clamav	0.99.2	All	All	All
Application	Clamav	Clamav	0.99.2	All	All	All

References

Reference	Source	Link
Bug 11798 – Clamav causes a use-after-free vulnerability when parsing PE files.	MISC	bugzilla.c
bb19798 - fix out of bound memory access for crafted wwunpack file. · Cisco-Talos/clamav-devel@dfc00cd · GitHub	MISC	github.co
ClamAV: Multiple vulnerabilities (GLSA 201804-16) — Gentoo security	GENTOO	security.g
varsleak-vul/clamav-use-after-free-pe.md at master · varsleak/varsleak-vul · GitHub	MISC	github.co
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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

© [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](#)