CVE-2007-2650

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2007-2650
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-05-14 21:19:00 UTC
Updated	2020-11-09 02:56:00 UTC
Description	The OLE2 parser in Clam AntiVirus (ClamAV) allows remote attackers to cause a denial of service (resource consumption)

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Clamav	Clamav	All	All	All	All
Application	Clamav	Clamav	All	All	All	All
Operating System	Debian	Debian Linux	3.1	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Operating System	Debian	Debian Linux	3.1	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All

References

Reference	Source	Link	Tags
ClamAV Multiple Vulnerabilities - Advisories - Secunia	SECUNIA	secunia.com	Patch, Third Party Ac
SUSE update for clamav - Advisories - Secunia	SECUNIA	secunia.com	Third Party Advisory
Clam AntiVirus ClamAV OLE2 Parser Remote Denial Of Service Vulnerability	BID	www.securityfocus.com	Third Party Advisory,
Trustix update for clamav - Advisories - Secunia	SECUNIA	secunia.com	Third Party Advisory
2007-0020	TRUSTIX	www.trustix.org	Broken Link
svn.clamav.net/svn/clamav-devel/trunk/ChangeLog	CONFIRM	svn.clamav.net	Broken Link
Mandriva update for clamav - Secunia.com	SECUNIA	secunia.com	Third Party Advisory
Debian -- Security Information -- DSA-1320-1 clamav	DEBIAN	www.debian.org	Third Party Advisory

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com	Permissions Require
404 Not Found	MLIST	lurker.clamav.net	Broken Link
ClamAV: Multiple Denials of Service — Gentoo Linux Documentation	GENTOO	security.gentoo.org	Third Party Advisory
Gmane -- Mail To News And Back Again	MISC	article.gmane.org	Broken Link
Gentoo update for clamav - Advisories - Secunia	SECUNIA	secunia.com	Third Party Advisory
Security Announcement	SUSE	www.novell.com	Third Party Advisory
Kolab Server ClamAV Denial of Service - Advisories - Secunia	SECUNIA	secunia.com	Third Party Advisory
404 Not Found	CONFIRM	kolab.org	Broken Link
Debian update for clamav - Advisories - Secunia	SECUNIA	secunia.com	Third Party Advisory
Support / Security / Advisories / / MDKSA-2007:115 | Mandriva	MANDRIVA	www.mandriva.com	Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

900004 CBL-Mariner Linux Security Update for clamav 0.101.2

903472 Common Base Linux Mariner (CBL-Mariner) Security Update for clamav (3170)

© 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 registred 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