CVE-2006-6406

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2006-6406
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-12-10 02:28:00 UTC
Updated	2018-10-17 21:48:00 UTC
Description	Clam AntiVirus (ClamAV) 0.88.6 allows remote attackers to bypass virus detection by inserting invalid characters into base6

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Clam Anti-virus	Clamav	0.88.6	All	All	All
Application	Clam Anti-virus	Clamav	0.88.6	All	All	All

References

Reference	Source	Link
Webmail - OVH	VUPEN	www.vupen.com
Webmail - OVH	VUPEN	www.vupen.com
Security Announcement	SUSE	www.novell.com
Mandriva update for clamav - Advisories - Secunia	SECUNIA	secunia.com
Debian -- Security Information -- DSA-1238-1 clamav	DEBIAN	www.debian.org
404 Not Found	CONFIRM	kolab.org
SUSE update for clamav - Advisories - Secunia	SECUNIA	secunia.com
Advisories - Mandriva Linux	MANDRIVA	www.mandriva.com
Debian update for clamav - Advisories - Secunia	SECUNIA	secunia.com
Multiple Security Products MIME Encoding Content Filter Bypass Weakness	BID	www.securityfocus.com
Kolab Server ClamAV Denial of Service Vulnerability - Advisories - Secunia	SECUNIA	secunia.com
Hendrik Weimer's Quantenblog - Security: Bypassing Virus Scanners Using MIME Encoding Tricks	MISC	www.quantenblog.net

SecurityFocus	BUGTRAQ	www.securityfocus.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.