CVE-2006-3815

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

Summary

CVE	CVE-2006-3815
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-07-25 13:22:00 UTC
Updated	2011-10-17 04:00:00 UTC
Description	heartbeat.c in heartbeat before 2.0.6 sets insecure permissions in a shmget call for shared memory, which allows local user

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Linux-ha	Heartbeat	All	All	All	All

References

Reference	Source	Link	Ta
Gentoo Linux Documentation -- Heartbeat: Denial of Service	GENTOO	security.gentoo.org	
Security Advisory SA21240 - Debian update for heartbeat - Secunia	SECUNIA	secunia.com	Ve
Secunia - Advisories - Ubuntu update for heartbeat	SECUNIA	secunia.com	Ve
SecurityTracker.com Archives - Heartbeat Shared Memory Error Lets Local Users Deny Service	SECTRACK	securitytracker.com	
CVS Repository - diff - Linux-HA: linux-ha/heartbeat/heartbeat.c	CONFIRM	cvs.linux-ha.org	Pa
Debian -- Security Information -- DSA-1128-1 heartbeat	DEBIAN	www.debian.org	
Advisories - Mandriva Linux	MANDRIVA	www.mandriva.com	
Heartbeat Shared Memory Insecure Permissions Denial of Service - Advisories - Secunia	SECUNIA	secunia.com	Ve
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com	Ve
Linux-ha-cvs Digest, Vol 32, Issue 43	CONFIRM	www.mail-archive.com	Pa
usn/usn-326-1 - Ubuntu: Linux for human beings	UBUNTU	www.ubuntu.com	
Gentoo update for heartbeat - Advisories - Secunia	SECUNIA	secunia.com	Ve
www.linux-ha.org/_cache/SecurityIssues__sec03.txt	CONFIRM	www.linux-ha.org	

Linux-HA Heartbeat Insecure Default Permissions on Shared Memory Vulnerability	BID	www.securityfocus.com	
Mandriva update for heartbeat - Secunia.com	SECUNIA	secunia.com	V
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**