CVE-2007-5730

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

Summary

CVE	CVE-2007-5730
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-10-30 22:46:00 UTC
Updated	2020-12-15 23:48:00 UTC
Description	Heap-based buffer overflow in QEMU 0.8.2, as used in Xen and possibly other products, allows local users to execute arbit

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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
Application	Qemu	Qemu	0.8.2	All	All	All
Application	Qemu	Qemu	0.8.2	All	All	All
Operating System	Xen	Xen	All	All	All	All
Operating System	Xen	Xen	All	All	All	All

References

Reference	Source	Link
taviso.decsystem.org/virtsec.pdf	MISC	taviso.decsystem.org
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
rhn.redhat.com | Red Hat Support	REDHAT	www.redhat.com
Debian update for qemu - Advisories - Secunia	SECUNIA	secunia.com
42985	OSVDB	osvdb.org
KVM Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.com

Support / Security / Advisories / / MDVSA-2008:162 | Mandriva	MANDRIVA	www.mandriva.com
QEMU Various Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
Red Hat update for xen - Advisories - Secunia	SECUNIA	secunia.com
Debian -- Security Information -- DSA-1284-1 qemu	DEBIAN	www.debian.org
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
QEMU Multiple Local Vulnerabilities	BID	www.securityfocus.com
Mandriva update for xen - Advisories - Secunia	SECUNIA	secunia.com
Support / Security / Advisories / / MDKSA-2007:203 | Mandriva	MANDRIVA	www.mandriva.com
Repository / Oval Repository	OVAL	oval.cisecurity.org
[VIM] Clarification on old QEMU/NE2000/Xen issues	VIM	www.attrition.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-11-02	Mark J Cox	Red Hat is aware of this issue and is tracking it via the following bug: https://bugzilla.redhat.com/

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