CVE-2008-4279

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

Summary

CVE	CVE-2008-4279
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-10-06 19:54:00 UTC
Updated	2018-11-02 13:06:00 UTC
Description	The CPU hardware emulation for 64-bit guest operating systems in VMware Workstation 6.0.x before 6.0.5 build 109488 ar

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Vmware	Esx	All	All	All	All
Application	Vmware	Player	All	All	All	All
Application	Vmware	Player	All	All	All	All
Application	Vmware	Server	All	All	All	All
Application	Vmware	Server	All	All	All	All
Application	Vmware	Workstation	All	All	All	All
Application	Vmware	Workstation	All	All	All	All

References

Reference	Source
IBM X-Force Exchange	XF
'VMSA-2008-0016 VMware Hosted products, VirtualCenter Update 3 and' - MARC	BUGTRAQ
SecurityFocus	BUGTRAQ
VMSA-2008-0016.2 - VMware	CONFIRM
VMware Products In-Guest Privilege Escalation and Information Disclosure Vulnerabilities	BID
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
[Full-disclosure] VMware Emulation Flaw x64 Guest Privilege Escalation (1/2)	FULLDISC

VMware ESX Server Sun Java JDK / JRE Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
Repository / Oval Repository	OVAL
VMware 64-bit Hardware Emulation Bug Lets Local Users Gain Elevated Privileges - SecurityTracker	SECTRAC
VMware ESX / ESXi "JMP" Privilege Escalation Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
VMware VirtualCenter Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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**