CVE-2015-4106

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

Summary

CVE	CVE-2015-4106
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-06-03 20:59:00 UTC
Updated	2020-09-09 15:15:00 UTC
Description	QEMU does not properly restrict write access to the PCI config space for certain PCI pass-through devices, which might all

Risk And Classification

Problem Types: CWE-863

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Application	Citrix	Xenserver	6.0	All	All	All
Application	Citrix	Xenserver	6.0.2	All	All	All
Application	Citrix	Xenserver	6.1.0	All	All	All
Application	Citrix	Xenserver	6.2.0	-	All	All
Application	Citrix	Xenserver	6.5	-	All	All
Application	Citrix	Xenserver	6.0	All	All	All
Application	Citrix	Xenserver	6.0.2	All	All	All
Application	Citrix	Xenserver	6.1.0	All	All	All
Application	Citrix	Xenserver	6.2.0	-	All	All

Application	Citrix	Xenserver	6.5	-	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Application	Qemu	Qemu	All	All	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp3	All	All
Operating System	Suse	Linux Enterprise Desktop	12	-	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp3	All	All
Operating System	Suse	Linux Enterprise Desktop	12	-	All	All
Operating System	Suse	Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	12	-	All	All
Operating System	Suse	Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	12	-	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11	sp3	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	-	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11	sp3	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	-	All	All

References

Reference
[SECURITY] Fedora 22 Update: xen-4.5.0-10.fc22
[SECURITY] Fedora 21 Update: xen-4.4.2-5.fc21
Xen CVE-2015-4106 Local Security Bypass Vulnerability
[security-announce] SUSE-SU-2015:1042-1: important: Security update for

[security-announce] SUSE-SU-2015:1156-1: important: Security update for
USN-2630-1: QEMU vulnerabilities | Ubuntu
Debian -- Security Information -- DSA-3286-1 xen
XSA-131 - Xen Security Advisories
Debian -- Security Information -- DSA-3284-1 qemu
[security-announce] SUSE-SU-2015:1157-1: important: Security update for
[SECURITY] Fedora 20 Update: xen-4.3.4-6.fc20
Xen: Multiple vulnerabilities (GLSA 201604-03) — Gentoo Security
Xen PCI Register Access Flaw Lets Local Users Obtain Potentially Sensitive Information, Gain Elevated Privileges, and Deny Service - Securi
[security-announce] SUSE-SU-2015:1045-1: important: Security update for
404 - Page not found
Citrix NetScaler Service Delivery Appliance Multiple Security Updates
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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