CVE-2014-1666

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

Summary

CVE	CVE-2014-1666
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-01-26 16:58:00 UTC
Updated	2018-01-03 02:29:00 UTC
Description	The do_physdev_op function in Xen 4.1.5, 4.1.6.1, 4.2.2 through 4.2.3, and 4.3.x does not properly restrict access to the (1

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Xen	Xen	4.1.5	All	All	All
Operating System	Xen	Xen	4.1.6.1	All	All	All
Operating System	Xen	Xen	4.2.2	All	All	All
Operating System	Xen	Xen	4.2.3	All	All	All
Operating System	Xen	Xen	4.3.0	All	All	All
Operating System	Xen	Xen	4.3.1	All	All	All
Operating System	Xen	Xen	4.1.5	All	All	All
Operating System	Xen	Xen	4.1.6.1	All	All	All
Operating System	Xen	Xen	4.2.2	All	All	All
Operating System	Xen	Xen	4.2.3	All	All	All
Operating System	Xen	Xen	4.3.0	All	All	All
Operating System	Xen	Xen	4.3.1	All	All	All

References

Reference
[security-announce] SUSE-SU-2014:0373-1: important: Security update for
Malformed Request

Security Advisory SA56650 - Xen "PHYSDEVOP_{prepare,release}_msix" Operations Security Bypass Security Issue - Secunia
XSA-87 - Xen Security Advisories
IBM X-Force Exchange
102536
Gentoo Linux Documentation -- Xen: Multiple Vunlerabilities
[SECURITY] Fedora 19 Update: xen-4.2.3-14.fc19
Citrix XenServer Multiple Security Updates
xenbits.xen.org/xsa/xsa87-unstable-4.3.patch
[SECURITY] Fedora 20 Update: xen-4.3.1-8.fc20
oss-security - Xen Security Advisory 87 (CVE-2014-1666) - PHYSDEVOP_{prepare,release}_msix exposed to unprivileged guests
Xen PHYSDEVOP_{prepare,release}_msix Access Control Flaw Lets Local Guest Users Deny Service on the Host - SecurityTracker
[security-announce] SUSE-SU-2014:0372-1: important: Security update for
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.