CVE-2015-7311

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

Summary

CVE	CVE-2015-7311
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-10-01 20:59:00 UTC
Updated	2018-10-30 16:26:00 UTC
Description	libxl in Xen 4.1.x through 4.6.x does not properly handle the readonly flag on disks when using the qemu-xen device model,

Risk And Classification

Problem Types: CWE-17

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Xen	Xen	4.1.0	All	All	All
Operating System	Xen	Xen	4.1.1	All	All	All
Operating System	Xen	Xen	4.1.2	All	All	All
Operating System	Xen	Xen	4.1.3	All	All	All
Operating System	Xen	Xen	4.1.4	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	4.2.0	All	All	All
Operating System	Xen	Xen	4.2.1	-	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	4.2.4	All	All	All
Operating System	Xen	Xen	4.2.5	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	4.3.2	All	All	All
Operating System	Xen	Xen	4.3.3	All	All	All

Operating System	Xen	Xen	4.3.4	All	All	All
Operating System	Xen	Xen	4.4.0	All	All	All
Operating System	Xen	Xen	4.4.0	rc1	All	All
Operating System	Xen	Xen	4.4.1	-	All	All
Operating System	Xen	Xen	4.5.0	All	All	All
Operating System	Xen	Xen	4.5.1	All	All	All
Operating System	Xen	Xen	4.1.0	All	All	All
Operating System	Xen	Xen	4.1.1	All	All	All
Operating System	Xen	Xen	4.1.2	All	All	All
Operating System	Xen	Xen	4.1.3	All	All	All
Operating System	Xen	Xen	4.1.4	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	4.2.0	All	All	All
Operating System	Xen	Xen	4.2.1	-	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	4.2.4	All	All	All
Operating System	Xen	Xen	4.2.5	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	4.3.2	All	All	All
Operating System	Xen	Xen	4.3.3	All	All	All
Operating System	Xen	Xen	4.3.4	All	All	All
Operating System	Xen	Xen	4.4.0	All	All	All
Operating System	Xen	Xen	4.4.0	rc1	All	All
Operating System	Xen	Xen	4.4.1	-	All	All
Operating System	Xen	Xen	4.5.0	All	All	All
Operating System	Xen	Xen	4.5.1	All	All	All

References

Reference	Source	
Xen libxl Read-Only Access Control Bypass Lets Local Users on a Guest System Write to the Target Disk - SecurityTracker	SECTRACK	
[SECURITY] Fedora 23 Update: xen-4.5.1-8.fc23	FEDORA	
Xen CVE-2015-7311 Security Bypass Vulnerability	BID	

[SECURITY] Fedora 22 Update: xen-4.5.1-8.fc22	FEDORA	
openSUSE-SU-2015:2250-1: moderate: Security update for xen	SUSE	
Debian -- Security Information -- DSA-3414-1 xen	DEBIAN	
[SECURITY] Fedora 21 Update: xen-4.4.3-3.fc21	FEDORA	
Xen: Multiple vulnerabilities (GLSA 201604-03) — Gentoo Security	GENTOO	
1257893 – Guests on Fedora22 Xen host are able to write to read-only disks with full device emulation type.	CONFIRM	
XSA-142 - Xen Security Advisories	CONFIRM	
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.