



# CVE-2015-2150

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2015-2150
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2015-03-12 14:59:00 UTC
<b>Updated</b>	2023-11-07 02:25:00 UTC
<b>Description</b>	Xen 3.3.x through 4.5.x and the Linux kernel through 3.19.1 do not properly restrict access to PCI command registers, which

## Risk And Classification

**Problem Types: CWE-264**

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Operating System	<a href="#">Ubuntu</a>	<a href="#">Ubuntu</a>	12.04	All	lts	All
Operating System	<a href="#">Ubuntu</a>	<a href="#">Ubuntu</a>	12.04	All	lts	All
Operating System	<a href="#">Xen</a>	<a href="#">Xen</a>	3.3.0	All	All	All
Operating System	<a href="#">Xen</a>	<a href="#">Xen</a>	3.3.1	All	All	All
Operating System	<a href="#">Xen</a>	<a href="#">Xen</a>	3.3.2	All	All	All
Operating System	<a href="#">Xen</a>	<a href="#">Xen</a>	3.4.0	All	All	All
Operating System	<a href="#">Xen</a>	<a href="#">Xen</a>	3.4.1	All	All	All
Operating System	<a href="#">Xen</a>	<a href="#">Xen</a>	3.4.2	All	All	All
Operating System	<a href="#">Xen</a>	<a href="#">Xen</a>	3.4.3	All	All	All
Operating System	<a href="#">Xen</a>	<a href="#">Xen</a>	3.4.4	All	All	All
Operating System	<a href="#">Xen</a>	<a href="#">Xen</a>	4.0.0	All	All	All
Operating System	<a href="#">Xen</a>	<a href="#">Xen</a>	4.0.1	All	All	All
Operating System	<a href="#">Xen</a>	<a href="#">Xen</a>	4.0.2	All	All	All
Operating System	<a href="#">Xen</a>	<a href="#">Xen</a>	4.0.3	All	All	All
Operating System	<a href="#">Xen</a>	<a href="#">Xen</a>	4.0.4	All	All	All
Operating System	<a href="#">Xen</a>	<a href="#">Xen</a>	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	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	4.4.0	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	3.3.0	All	All	All
Operating System	Xen	Xen	3.3.1	All	All	All
Operating System	Xen	Xen	3.3.2	All	All	All
Operating System	Xen	Xen	3.4.0	All	All	All
Operating System	Xen	Xen	3.4.1	All	All	All
Operating System	Xen	Xen	3.4.2	All	All	All
Operating System	Xen	Xen	3.4.3	All	All	All
Operating System	Xen	Xen	3.4.4	All	All	All
Operating System	Xen	Xen	4.0.0	All	All	All
Operating System	Xen	Xen	4.0.1	All	All	All
Operating System	Xen	Xen	4.0.2	All	All	All
Operating System	Xen	Xen	4.0.3	All	All	All
Operating System	Xen	Xen	4.0.4	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	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	4.4.0	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

## References

Reference	Source
[SECURITY] Fedora 20 Update: kernel-3.19.4-100.fc20	FEDORA
XSA-120 - Xen Security Advisories	CONFIRM
USN-2631-1: Linux kernel vulnerabilities   Ubuntu	UBUNTU
Debian -- Security Information -- DSA-3237-1 linux	DEBIAN
xen-pciback: limit guest control of command register · torvalds/linux@af6fc85 · GitHub	CONFIRM
[security-announce] SUSE-SU-2015:0658-1: important: Security Update for	SUSE
[security-announce] SUSE-SU-2015:1478-1: important: Security update for	SUSE
Xen Non-maskable Interrupt Generation Lets Local Guest Users Crash the Host System - SecurityTracker	SECTRACK
[security-announce] SUSE-SU-2015:1611-1: important: Security update for	SUSE
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM
[SECURITY] Fedora 22 Update: kernel-4.0.0-1.fc22	FEDORA
Security_Advisory-Xen Vulnerabilities on Huawei FusionSphere products - Huawei PSIRT	CONFIRM
Oracle Linux Bulletin - January 2016	CONFIRM
Bugtraq: [SECURITY] [DSA 4497-1] linux security update	BUGTRAQ
Bug 1196266 – CVE-2015-2150 CVE-2015-8553 xen: non-maskable interrupts triggerable by guests (xsa120)	CONFIRM
kernel/git/torvalds/linux.git - Linux kernel source tree	
Xen CVE-2015-2150 Denial of Service Vulnerability	BID
[security-announce] SUSE-SU-2015:1592-1: important: Security update for	SUSE
[SECURITY] Fedora 21 Update: kernel-3.19.4-200.fc21	FEDORA
USN-2632-1: Linux kernel (OMAP4) vulnerabilities   Ubuntu	UBUNTU
[SECURITY] Fedora 22 Update: kernel-4.0.0-0.rc4.git0.1.fc22	FEDORA
Xen Multiple Flaws Let Local Guest Users Deny Service or Obtain Information From Other Guest Systems - SecurityTracker	SECTRACK

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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**