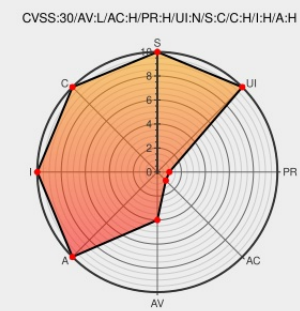
CVE-2015-8554

Published on: 04/14/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:14 PM UTC

CVE-2015-8554

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Xen from Xen contain the following vulnerability:

Buffer overflow in hw/pt-msi.c in Xen 4.6.x and earlier, when using the qemu-xen-traditional (aka qemu-dm) device model, allows local x86 HVM guest administrators to gain privileges by leveraging a system with access to a passed-through MSI-X capable physical PCI device and MSI-X table entries, related to a "write path."

CVE-2015-8554 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	HIGH	HIGH	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.6 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Xen 'pt-msi.c' Heap Memory Corruption Vulnerability	cve.report (archive) text/html	BID 79579
XSA-164 - Xen Security Advisories	Vendor Advisory xenbits.xen.org	CONFIRM xenbits.xen.org/xsa/advisory-164.html

	text/html	
Citrix XenServer Multiple Security Updates	Vendor Advisory support.citrix.com text/html	CONFIRM support.citrix.com/article/CTX203879
Oracle VM Server for x86 Bulletin - July 2016	web.archive.org text/html Inactive Link Not Archived	CONFIRM www.oracle.com/technetwork/topics/security/ovmbulletinjul2016-3090546.html
Xen: Multiple vulnerabilities (GLSA 201604-03) — Gentoo Security	security.gentoo.org text/html	GENTOO GLSA-201604-03
Xen Buffer Overflow in qemu-dm Lets Local Administrative Users on a Guest System Gain Elevated Privileges on the Host System - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1034481

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Xen	Xen	All	All	All	All

cpe:2.3:o:xen:xen:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→