CVE-2014-7188

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

Summary

CVE	CVE-2014-7188
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-10-02 14:55:05 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The hvm_msr_read_intercept function in arch/x86/hvm/hvm.c in Xen 4.1 through 4.4.x uses an improper MSR range for x2/

Risk And Classification

Primary CVSS: v2.0 8.3 from nvd@nist.gov

AV:A/AC:L/Au:N/C:C/I:C/A:C

Problem Types: CWE-399 | n/a

CVSS v2.0 Breakdown

Access Vector

Adjacent

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:A/AC:L/Au:N/C:C/I:C/A:C

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	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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Sou
[security-announce] openSUSE-SU-2014:1281-1: important: xen: security an	af85
Malformed Request	af85
www.c7zero.info/stuff/csw2017_ExploringYourSystemDeeper_updated.pdf	af85
XSA-108 - Xen Security Advisories	af85
Security Advisory SA61664 - Xen x2APIC Emulation MSR Access Information Disclosure and Denial of Service Vulnerability - Secunia	af85
Xen: Denial of Service (GLSA 201412-42) — Gentoo security	af85
Citrix XenServer Multiple Security Updates	af85
IBM X-Force Exchange	af85
[SECURITY] Fedora 20 Update: xen-4.3.3-3.fc20	af85
404 - Page not found	af85
Xen x2APIC Emulation Flaw Lets Local Guest Systems Obtain Data from Other Guest Systems or the Host System - SecurityTracker	af85
Debian -- Security Information -- DSA-3041-1 xen	af85
Security Advisory SA61890 - Gentoo update for xen - Secunia	af85
[security-announce] openSUSE-SU-2014:1279-1: important: xen: security an	af85
[SECURITY] Fedora 19 Update: xen-4.2.5-3.fc19	af85

[SECURITY] Fedora 19 Update: xen-4.2.5-3.fc19	af85
[SECURITY] Fedora 21 Update: xen-4.4.1-6.fc21	af85
Security Advisory SA61858 - Citrix XenServer Multiple Vulnerabilities - Secunia	af85
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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