



CVE-2015-4164

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

Summary

CVE	CVE-2015-4164
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-06-15 15:59:13 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The compat_iret function in Xen 3.1 through 4.5 iterates the wrong way through a loop, which allows local 32-bit PV guest a

Risk And Classification

Primary CVSS: v2.0 4.9 from nvd@nist.gov

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

Problem Types: CWE-399 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Xen	Xen	3.1.3	All	All	All

Operating System	Xen	Xen	3.1.4	All	All	All
Operating System	Xen	Xen	3.2.0	All	All	All
Operating System	Xen	Xen	3.2.1	All	All	All
Operating System	Xen	Xen	3.2.2	All	All	All
Operating System	Xen	Xen	3.2.3	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	4.3.4	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

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

References	
Reference	Source
[security-announce] SUSE-SU-2015:1206-1: important: Security update for	af854a3a-2127-422b-91ae-36
Xen Logic Error in compat_iret() Lets Local Guest Users Deny Service on the Host System - SecurityTracker	af854a3a-2127-422b-91ae-36
[security-announce] SUSE-SU-2015:1643-1: important: Security update for	af854a3a-2127-422b-91ae-36
[security-announce] SUSE-SU-2015:1045-1: important: Security update for	af854a3a-2127-422b-91ae-36
[security-announce] SUSE-SU-2015:1157-1: important: Security update for	af854a3a-2127-422b-91ae-36
Debian -- Security Information -- DSA-3286-1 xen	af854a3a-2127-422b-91ae-36
XSA-136 - Xen Security Advisories	af854a3a-2127-422b-91ae-36
Xen CVE-2015-4164 Local Denial of Service Vulnerability	af854a3a-2127-422b-91ae-36
[security-announce] SUSE-SU-2015:1042-1: important: Security update for	af854a3a-2127-422b-91ae-36
404 - Page not found	af854a3a-2127-422b-91ae-36
[security-announce] SUSE-SU-2015:1156-1: important: Security update for	af854a3a-2127-422b-91ae-36
Xen: Multiple vulnerabilities (GLSA 201604-03) — Gentoo Security	af854a3a-2127-422b-91ae-36
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.