CVE-2016-3961

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

Summary

CVE	CVE-2016-3961
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-04-15 14:59:14 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Xen and the Linux kernel through 4.5.x do not properly suppress hugetlbfs support in x86 PV guests, which allows local PV

Risk And Classification

Primary CVSS: v3.0 5.5 MEDIUM from nvd@nist.gov

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

Problem Types: CWE-20 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	5.5	MEDIUM	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
2.0	nvd@nist.gov	Primary	2.1		AV:L/AC:L/Au:N/C:N/I:N/A:P

CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Xen	Xen	All	All	All	All

Vendor Declared Affected Products

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

References

Reference	So
XSA-174 - Xen Security Advisories	af8
Xen CVE-2016-3961 Denial of Service Vulnerability	af8
USN-3007-1: Linux kernel (Raspberry Pi 2) vulnerabilities | Ubuntu	af8
USN-3002-1: Linux kernel (Wily HWE) vulnerabilities | Ubuntu	af8
USN-3005-1: Linux kernel (Xenial HWE) vulnerabilities | Ubuntu	af8
Debian -- Security Information -- DSA-3607-1 linux	af8
USN-3050-1: Linux kernel (OMAP4) vulnerabilities | Ubuntu	af8

USN-3003-1: Linux kernel vulnerabilities | Ubuntu	af8
Xen hugetlbfs Support Lets Local Users on a Guest System Cause Denial of Service Conditions on the Guest System - SecurityTracker	af8
USN-3004-1: Linux kernel (Raspberry Pi 2) vulnerabilities | Ubuntu	af8
USN-3049-1: Linux kernel vulnerabilities | Ubuntu	af8
USN-3001-1: Linux kernel (Vivid HWE) vulnerabilities | Ubuntu	af8
USN-3006-1: Linux kernel vulnerabilities | Ubuntu	af8
xenbits.xen.org/xsa/xsa174.patch	af8
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**