



CVE-2016-1570

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

Summary

CVE	CVE-2016-1570
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-01-22 15:59:05 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The PV superpage functionality in arch/x86/mm.c in Xen 3.4.0, 3.4.1, and 4.1.x through 4.6.x allows local PV guests to obtain kernel memory addresses and execute arbitrary code.

Risk And Classification

Primary CVSS: v3.0 8.5 HIGH from nvd@nist.gov

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

Problem Types: CWE-20 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	8.5	HIGH	CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	6.9		AV:L/AC:M/Au:N/C:C/I:C/A:C

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

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

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:L/AC:M/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	3.4.0	All	All	All
Operating System	Xen	Xen	3.4.1	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	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	4.2.4	All	All	All
Operating System	Xen	Xen	4.2.5	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	4.3.2	All	All	All
Operating System	Xen	Xen	4.3.3	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	All
Operating System	Xen	Xen	4.4.2	All	All	All
Operating System	Xen	Xen	4.4.3	All	All	All
Operating System	Xen	Xen	4.5.0	All	All	All
Operating System	Xen	Xen	4.5.1	All	All	All
Operating System	Xen	Xen	4.5.2	All	All	All
Operating System	Xen	Xen	4.6.0	All	All	All

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

References	
Reference	Source
Debian -- Security Information -- DSA-3519-1 xen	af854a:
Xen PV Superpage Hypercalls Lets Local Users on a Guest System Gain Elevated Privileges on the Host System - SecurityTracker	af854a:
XSA-167 - Xen Security Advisories	af854a:
CVE Program record	CVE.O
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

