CVE-2016-7777

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

Summary

CVE	CVE-2016-7777
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-10-07 14:59:10 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Xen 4.7.x and earlier does not properly honor CR0.TS and CR0.EM, which allows local x86 HVM guest OS users to read o

Risk And Classification

Primary CVSS: v3.0 6.3 MEDIUM from nvd@nist.gov

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

EPSS: 0.001220000 probability, percentile 0.307870000 (date 2026-05-07)

Problem Types: CWE-362 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	6.3	MEDIUM	CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N
2.0	nvd@nist.gov	Primary	3.3		AV:L/AC:M/Au:N/C:P/I:P/A:N

CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

High

Availability

None

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

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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
Xen Control Register Access Race Condition Lets Local Users on a Guest System Read or Modify Register State Data for Other Processes or
CVE-2016-7777 - Citrix XenServer Security Update
XSA-190 - Xen Security Advisories
Xen CVE-2016-7777 Security Bypass Vulnerability
Xen: Multiple vulnerabilities (GLSA 201611-09) — Gentoo security
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

500809 Alpine Linux Security Update for xen

504552 Alpine Linux Security Update for xen