Use after free of paging structures in EPT

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

Summary

CVE	CVE-2026-23554
State	PUBLISHED
Assigner	XEN
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-23 07:16:07 UTC
Updated	2026-04-10 20:40:33 UTC
Description	The Intel EPT paging code uses an optimization to defer flushing of any cached EPT state until the p2m lock is dropped, so

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from ADP

CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

EPSS: 0.000120000 probability, percentile 0.015830000 (date 2026-04-15)

Problem Types: CWE-367 | CWE-367 CWE-367 Time-of-check Time-of-use (TOCTOU) Race Condition

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

High

ntegrity

High

Availability

High

CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

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	Xen	Xen	unknown consult Xen advisory XSA-480	Not specified

References

Reference	Source	Link	Tags
www.openwall.com/lists/oss-security/2026/03/17/6	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	Mailing List, Patch
xenbits.xen.org/xsa/advisory-480.html	af854a3a-2127-422b-91ae-364da2661108	xenbits.xen.org	Patch, Vendor Adv
xenbits.xenproject.org/xsa/advisory-480.html	security@xen.org	xenbits.xenproject.org	Patch, Vendor Adv
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: This issue was discovered by Roger Pau Monné of XenServer. (en)

Additional Advisory Data

Workarounds

CNA: There are no mitigations.

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**