Xenstored DoS by unprivileged domain

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

Summary

CVE	CVE-2026-23555
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 20:38:17 UTC
Description	Any guest issuing a Xenstore command accessing a node using the (illegal) node path "/local/domain/", will crash xenstored

Risk And Classification

Primary CVSS: v3.1 7.1 HIGH from nvd@nist.gov

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

EPSS: 0.000150000 probability, percentile 0.032650000 (date 2026-04-15)

Problem Types: CWE-617 | CWE-617 CWE-617 Reachable Assertion

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.1	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H
3.1	ADP	DECLARED	7.1	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.1	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

None

ntegrity

None

Availability

High

CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:N/I:N/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-481	Not specified

References

Reference	Source	Link	Tags
www.openwall.com/lists/oss-security/2026/03/17/7	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	Mailing List, Patch,
xenbits.xenproject.org/xsa/advisory-481.html	security@xen.org	xenbits.xenproject.org	Patch, Vendor Adv
xenbits.xen.org/xsa/advisory-481.html	af854a3a-2127-422b-91ae-364da2661108	xenbits.xen.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 Marek Marczykowski-Góreckiof Invisible Things Lab. (en)

Additional Advisory Data

Workarounds

CNA: There is no known mitigation available.

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**