



CVE-2022-42321

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2022-42321
State	PUBLIC
Assigner	security@xen.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-01 13:15:00 UTC
Updated	2024-02-04 08:15:00 UTC
Description	Xenstore: Guests can crash xenstored via exhausting the stack Xenstored is using recursion for some Xenstore operations

Risk And Classification

Problem Types: CWE-674

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Operating System	Fedoraproject	Fedora	37	All	All	All
Operating System	Xen	Xen	-	All	All	All

References

Reference	Source
[SECURITY] Fedora 37 Update: xen-4.16.2-4.fc37 - package-announce - Fedora Mailing-Lists	FEDORA
oss-security - Xen Security Advisory 418 v2 (CVE-2022-42321) - Xenstore: Guests can crash xenstored via exhausting the stack	MLIST
XSA-418 - Xen Security Advisories	CONFIRM
xenbits.xenproject.org/xsa/advisory-418.txt	MISC
Xen: Multiple Vulnerabilities (GLSA 202402-07) — Gentoo security	
[SECURITY] Fedora 37 Update: xen-4.16.2-4.fc37 - package-announce - Fedora Mailing-Lists	
Debian -- Security Information -- DSA-5272-1 xen	DEBIAN
[SECURITY] Fedora 36 Update: xen-4.16.2-3.fc36 - package-announce - Fedora Mailing-Lists	
[SECURITY] Fedora 36 Update: xen-4.16.2-3.fc36 - package-announce - Fedora Mailing-Lists	FEDORA

[SECURITY] Fedora 35 Update: xen-4.15.3-7.fc35 - package-announce - Fedora Mailing-Lists

FEDORA

[SECURITY] Fedora 35 Update: xen-4.15.3-7.fc35 - package-announce - Fedora Mailing-Lists

CVE Program record

CVE.ORG

NVD vulnerability detail

NVD

Vendor Comments And Credit

Discovery Credit

LEGACY: Array

Legacy QID Mappings

[181193](#) Debian Security Update for xen (DSA 5272-1)

[183439](#) Debian Security Update for xen (CVE-2022-42321)

[283293](#) Fedora Security Update for xen (FEDORA-2022-07438e12df)

[283319](#) Fedora Security Update for xen (FEDORA-2022-99af00f60e)

[283430](#) Fedora Security Update for xen (FEDORA-2022-9f51d13fa3)

[390275](#) Oracle Managed Virtualization (VM) Server for x86 Security Update for xen (OVMSA-2023-0005)

[502600](#) Alpine Linux Security Update for xen

[502619](#) Alpine Linux Security Update for xen

[503143](#) Alpine Linux Security Update for xen

[503695](#) Alpine Linux Security Update for xen

[504549](#) Alpine Linux Security Update for xen

[505964](#) Alpine Linux Security Update for xen

[710858](#) Gentoo Linux Xen Multiple Vulnerabilities (GLSA 202402-07)

[752778](#) SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:3925-1)

[752781](#) SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:3928-1)

[752792](#) SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:3947-1)

[752796](#) SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:3971-1)

[752807](#) SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:4007-1)

[752887](#) SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:4241-1)

[752979](#) SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:4332-1)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)