



CVE-2022-33746

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

Summary

CVE	CVE-2022-33746
State	PUBLIC
Assigner	security@xen.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-10-11 13:15:00 UTC
Updated	2024-02-04 08:15:00 UTC
Description	P2M pool freeing may take excessively long The P2M pool backing second level address translation for guests may be of s

Risk And Classification

Problem Types: CWE-404

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	All

References

Reference	Source	Link
[SECURITY] Fedora 36 Update: xen-4.16.2-2.fc36 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
XSA-410 - Xen Security Advisories	CONFIRM	xenbits.xen.org
[SECURITY] Fedora 37 Update: xen-4.16.2-2.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
Xen: Multiple Vulnerabilities (GLSA 202402-07) — Gentoo security		security.gentoo.org
Debian -- Security Information -- DSA-5272-1 xen	DEBIAN	www.debian.org
oss-security - Xen Security Advisory 410 v3 (CVE-2022-33746) - P2M pool freeing may take excessively long	MLIST	www.openwall.com
[SECURITY] Fedora 36 Update: xen-4.16.2-2.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
xenbits.xenproject.org/xsa/advisory-410.txt	MISC	xenbits.xenproject.org
[SECURITY] Fedora 37 Update: xen-4.16.2-2.fc37 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org

[SECURITY] Fedora 35 Update: xen-4.15.3-7.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 35 Update: xen-4.15.3-7.fc35 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit
LEGACY: Array

Legacy QID Mappings

181193 Debian Security Update for xen (DSA 5272-1)
182954 Debian Security Update for xen (CVE-2022-33746)
283267 Fedora Security Update for xen (FEDORA-2022-5b594b82ac)
283319 Fedora Security Update for xen (FEDORA-2022-99af00f60e)
283476 Fedora Security Update for xen (FEDORA-2022-d80cc73088)
390270 Oracle VM Server for x86 Security Update for xen (OVMSA-2022-0029)
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)
752684 SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:3665-1)
752715 SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:3727-1)
752719 SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:3728-1)
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)

© [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](#)