



CVE-2022-26362

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2022-26362
State	PUBLIC
Assigner	security@xen.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-06-09 17:15:00 UTC
Updated	2023-11-07 03:44:00 UTC
Description	x86 pv: Race condition in typeref acquisition Xen maintains a type reference count for pages, in addition to a regular referer

Risk And Classification

Problem Types: CWE-362

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	Xen	Xen	All	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 36 Update: qemu-6.2.0-12.fc36 - package-announce - Fedora Mailing-Lists		lists.fedoraproje
oss-security - Xen Security Advisory 401 v2 (CVE-2022-26362) - x86 pv: Race condition in typeref acquisition	MLIST	www.openwall.c
XSA-401 - Xen Security Advisories	CONFIRM	xenbits.xen.org
[SECURITY] Fedora 35 Update: xen-4.15.3-2.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproje
Xen: Multiple Vulnerabilities (GLSA 202208-23) — Gentoo security	GENTOO	security.gentoo.
[SECURITY] Fedora 35 Update: xen-4.15.3-2.fc35 - package-announce - Fedora Mailing-Lists		lists.fedoraproje
xenbits.xenproject.org/xsa/advisory-401.txt	MISC	xenbits.xenproj
Debian -- Security Information -- DSA-5184-1 xen	DEBIAN	www.debian.org
[SECURITY] Fedora 36 Update: qemu-6.2.0-12.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproje
Xen TLB Flush Bypass ≈ Packet Storm	MISC	packetstormsec

Vendor Comments And Credit

Discovery Credit

LEGACY: Array

Legacy QID Mappings

180893 Debian Security Update for xen (DSA 5184-1)
182358 Debian Security Update for xen (CVE-2022-26362)
282863 Fedora Security Update for collectd (FEDORA-2022-0142d562ca)
282969 Fedora Security Update for xen (FEDORA-2022-2c9f8224f8)
377772 Citrix XenServer Security Updates (CTX460064)
501524 Alpine Linux Security Update for xen
501802 Alpine Linux Security Update for xen
502243 Alpine Linux Security Update for xen
502812 Alpine Linux Security Update for xen
710600 Gentoo Linux Xen Multiple Vulnerabilities (GLSA 202208-23)
752227 SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:2065-1)
752238 SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:2084-1)
752262 SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:2158-1)
752264 SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:2164-1)
752299 SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:2296-1)
752395 SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:2560-1)
752399 SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:2601-1)
752400 SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:2600-1)
752405 SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:2599-1)
752410 SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:2597-1)
752411 SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:2591-1)

© [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](#)