



# CVE-2022-26364

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2022-26364
<b>State</b>	PUBLIC
<b>Assigner</b>	security@xen.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-06-09 17:15:00 UTC
<b>Updated</b>	2023-11-07 03:44:00 UTC
<b>Description</b>	x86 pv: Insufficient care with non-coherent mappings T[his CNA information record relates to multiple CVEs; the text explain

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	11.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	35	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	36	All	All	All
Operating System	<a href="#">Xen</a>	<a href="#">Xen</a>	All	All	All	All

## References

Reference	Sc
[SECURITY] Fedora 36 Update: qemu-6.2.0-12.fc36 - package-announce - Fedora Mailing-Lists	
[SECURITY] Fedora 35 Update: xen-4.15.3-2.fc35 - package-announce - Fedora Mailing-Lists	FE
Xen: Multiple Vulnerabilities (GLSA 202208-23) — Gentoo security	GI
xenbits.xenproject.org/xsa/advisory-402.txt	MI
XSA-402 - Xen Security Advisories	CC
[SECURITY] Fedora 35 Update: xen-4.15.3-2.fc35 - package-announce - Fedora Mailing-Lists	
Debian -- Security Information -- DSA-5184-1 xen	DE
oss-security - Xen Security Advisory 402 v4 (CVE-2022-26363,CVE-2022-26364) - x86 pv: Insufficient care with non-coherent mappings	MI
Xen PV Guest Non-SELF Snooping CPU Memory Corruption ≈ Packet Storm	MI
[SECURITY] Fedora 36 Update: qemu-6.2.0-12.fc36 - package-announce - Fedora Mailing-Lists	FE

## Vendor Comments And Credit

Discovery Credit

**LEGACY: Array**

## Legacy QID Mappings

180893	Debian Security Update for xen (DSA 5184-1)
184988	Debian Security Update for xen (CVE-2022-26364)
282863	Fedora Security Update for collectd (FEDORA-2022-0142d562ca)
282969	Fedora Security Update for xen (FEDORA-2022-2c9f8224f8)
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)
752781	SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:3928-1)

© [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](#)**