



CVE-2022-26356

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

Summary

CVE	CVE-2022-26356
State	PUBLIC
Assigner	security@xen.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-05 13:15:00 UTC
Updated	2024-02-04 08:15:00 UTC
Description	Racy interactions between dirty vram tracking and paging log dirty hypercalls Activation of log dirty mode done by XEN_DM

Risk And Classification

Problem Types: CWE-667

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	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Xen	Xen	All	All	All	All

References

Reference
Debian -- Security Information -- DSA-5117-1 xen
[SECURITY] Fedora 35 Update: xen-4.15.2-3.fc35 - package-announce - Fedora Mailing-Lists
Xen: Multiple Vulnerabilities (GLSA 202402-07) — Gentoo security
oss-security - Xen Security Advisory 397 v2 (CVE-2022-26356) - Racy interactions between dirty vram tracking and paging log dirty hypercalls
[SECURITY] Fedora 34 Update: xen-4.14.5-1.fc34 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 35 Update: xen-4.15.2-3.fc35 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 34 Update: xen-4.14.5-1.fc34 - package-announce - Fedora Mailing-Lists
xenbits.xenproject.org/xsa/advisory-397.txt
XSA-397 - Xen Security Advisories
CVE Program record

Vendor Comments And Credit

Discovery Credit

LEGACY: Array

Legacy QID Mappings

179182 Debian Security Update for xen (DSA 5117-1)
184860 Debian Security Update for xen (CVE-2022-26356)
282617 Fedora Security Update for xen (FEDORA-2022-dfbf7e2372)
282643 Fedora Security Update for xen (FEDORA-2022-64b2c02d29)
390260 Oracle Managed Virtualization (VM) Server for x86 Security Update for xen (OVMSA-2022-0012)
500806 Alpine Linux Security Update for xen
501523 Alpine Linux Security Update for xen
502242 Alpine Linux Security Update for xen
502421 Alpine Linux Security Update for xen
504548 Alpine Linux Security Update for xen
710858 Gentoo Linux Xen Multiple Vulnerabilities (GLSA 202402-07)
752054 SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:1285-1)
752065 SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:1300-1)
752073 SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:1359-1)
752075 SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:1408-1)
752099 SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:1506-1)
752100 SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:1505-1)
752262 SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:2158-1)

© [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](#)