



CVE-2021-28702

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2021-28702 |
| State | PUBLIC |
| Assigner | security@xen.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2021-10-06 14:15:00 UTC |
| Updated | 2023-11-07 03:32:00 UTC |
| Description | PCI devices with RMRRs not deassigned correctly Certain PCI devices in a system might be assigned Reserved Memory F |

Risk And Classification

Problem Types: CWE-269

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|-------------------------------|------------------------------|---------|--------|---------|----------|
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Operating System | Fedoraproject | Fedora | 33 | 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 | Source | Link |
|--|--------|-----------------------------|
| [SECURITY] Fedora 35 Update: xen-4.15.1-2.fc35 - package-announce - Fedora Mailing-Lists | | lists.fedor |
| oss-security - Xen Security Advisory 386 v2 (CVE-2021-28702) - PCI devices with RMRRs not deassigned correctly | MLIST | www.oper |
| Xen: Multiple Vulnerabilities (GLSA 202208-23) — Gentoo security | GENTOO | security.g |
| [SECURITY] Fedora 33 Update: xen-4.14.3-2.fc33 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedor |
| [SECURITY] Fedora 34 Update: xen-4.14.3-2.fc34 - package-announce - Fedora Mailing-Lists | | lists.fedor |
| [SECURITY] Fedora 33 Update: xen-4.14.3-2.fc33 - package-announce - Fedora Mailing-Lists | | lists.fedor |
| Debian -- Security Information -- DSA-5017-1 xen | DEBIAN | www.debi |
| [SECURITY] Fedora 35 Update: xen-4.15.1-2.fc35 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedor |
| [SECURITY] Fedora 34 Update: xen-4.14.3-2.fc34 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedor |

| | | |
|---|---------|--|
| xenbits.xenproject.org/xsa/advisory-386.txt | MISC | xenbits.xe |
| CVE Program record | CVE.ORG | www.cve.o |
| NVD vulnerability detail | NVD | nvd.nist.g |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

| |
|--|
| 184281 Debian Security Update for xen (CVE-2021-28702) |
| 281988 Fedora Security Update for xen (FEDORA-2021-0b7a484688) |
| 281989 Fedora Security Update for xen (FEDORA-2021-80bbe7def0) |
| 500804 Alpine Linux Security Update for xen |
| 501521 Alpine Linux Security Update for xen |
| 501799 Alpine Linux Security Update for xen |
| 502458 Alpine Linux Security Update for xen |
| 504546 Alpine Linux Security Update for xen |
| 710600 Gentoo Linux Xen Multiple Vulnerabilities (GLSA 202208-23) |
| 751411 SUSE Enterprise Linux Security Update for xen (SUSE-SU-2021:3852-1) |
| 751454 OpenSUSE Security Update for xen (openSUSE-SU-2021:1543-1) |
| 751474 OpenSUSE Security Update for xen (openSUSE-SU-2021:3968-1) |
| 751477 SUSE Enterprise Linux Security Update for xen (SUSE-SU-2021:3977-1) |

© [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](#)