



# CVE-2017-7228

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2017-7228  |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | cve@mitre.org  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2017-04-04 14:59:00 UTC  |
| <b>Updated</b>         | 2019-10-03 00:03:00 UTC  |
| <b>Description</b>     | An issue (known as XSA-212) was discovered in Xen, with fixes available for 4.8.x, 4.7.x, 4.6.x, 4.5.x, and 4.4.x. The earlier |

## Risk And Classification

**Problem Types:** CWE-129

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor | Product | Version | Update | Edition | Language |
|------------------|--------|---------|---------|--------|---------|----------|
| Operating System | Xen    | Xen     | -       | All    | All     | All      |
| Operating System | Xen    | Xen     | -       | All    | All     | All      |

## References

### Reference

|   |
|---|
| Xen 'memory_exchange()' Function Incomplete Fix Privilege Escalation Vulnerability  |
| qubes-secpack/qsbs-029-2017.txt at master · QubesOS/qubes-secpack · GitHub  |
| Xen - Broken Check in 'memory_exchange()' Permits PV Guest Breakout   |
| oss-security - Xen Security Advisory 212 (CVE-2017-7228) - x86: broken check in memory_exchange() permits PV guest breakout         |
| Debian -- Security Information -- DSA-3847-1 xen  |
| Project Zero: Pandavirtualization: Exploiting the Xen hypervisor  |
| Xen XENMEM_exchange Validation Flaw Lets Local Users on a Guest System Gain Elevated Privileges on the Host System - SecurityTracke |
| XSA-212 - Xen Security Advisories   |
| CVE Program record  |
| NVD vulnerability detail  |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

500814 Alpine Linux Security Update for xen

504557 Alpine Linux Security Update for xen

510417 Alpine Linux Security Update for xen

© [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](#)