



# CVE-2017-10920

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

## Summary

|                        |                                                                                                               |
|------------------------|---------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2017-10920                                                                                                |
| <b>State</b>           | PUBLIC                                                                                                        |
| <b>Assigner</b>        | cve@mitre.org                                                                                                 |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                  |
| <b>Published</b>       | 2017-07-05 01:29:00 UTC                                                                                       |
| <b>Updated</b>         | 2019-10-03 00:03:00 UTC                                                                                       |
| <b>Description</b>     | The grant-table feature in Xen through 4.8.x mishandles a GNTMAP_device_map and GNTMAP_host_map mapping, wher |

## Risk And Classification

### Problem Types: CWE-119

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor              | Product             | Version | Update | Edition | Language |
|------------------|---------------------|---------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Xen</a> | <a href="#">Xen</a> | All     | All    | All     | All      |

## References

| Reference                                                                                                                    | Source |
|------------------------------------------------------------------------------------------------------------------------------|--------|
| Xen Grant Table Mapping Bugs Let Local Users on a Guest System Gain Elevated Privileges on the Host System - SecurityTracker | SECTF  |
| XSA-224 - Xen Security Advisories                                                                                            | CONFI  |
| Xen: Multiple vulnerabilities (GLSA 201710-17) — Gentoo security                                                             | GENTC  |
| Gentoo Linux — Error 404 (Not Found)                                                                                         | GENTC  |
| Debian -- Security Information -- DSA-3969-1 xen                                                                             | DEBIA  |
| CVE Program record                                                                                                           | CVE.O  |
| NVD vulnerability detail                                                                                                     | NVD    |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[500816](#) Alpine Linux Security Update for xen

[504559](#) 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](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)