



CVE-2017-12137

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

Summary

CVE	CVE-2017-12137
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-24 14:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	arch/x86/mm.c in Xen allows local PV guest OS users to gain host OS privileges via vectors related to map_grant_ref.

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Citrix	Xenserver	6.0.2	All	All	All
Application	Citrix	Xenserver	6.2.0	All	All	All
Application	Citrix	Xenserver	6.5	All	All	All
Application	Citrix	Xenserver	7.0	All	All	All
Application	Citrix	Xenserver	7.1	All	All	All
Application	Citrix	Xenserver	7.2	All	All	All
Application	Citrix	Xenserver	6.0.2	All	All	All
Application	Citrix	Xenserver	6.2.0	All	All	All
Application	Citrix	Xenserver	6.5	All	All	All
Application	Citrix	Xenserver	7.0	All	All	All
Application	Citrix	Xenserver	7.1	All	All	All
Application	Citrix	Xenserver	7.2	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Xen	Xen	All	All	All	All

Operating System Xen Xen All All All All

References

Reference

1477657 – (CVE-2017-12137, xsa227) CVE-2017-12137 xsa227 xen: x86: PV privilege escalation via map_grant_ref (XSA-227)

Xen: Multiple vulnerabilities (GLSA 201801-14) — Gentoo security

XSA-227 - Xen Security Advisories

Xen CVE-2017-12137 Privilege Escalation Vulnerability

oss-security - Xen Security Advisory 227 (CVE-2017-12137) - x86: PV privilege escalation via map_grant_ref

Citrix XenServer Multiple Security Updates

Debian -- Security Information -- DSA-3969-1 xen

Xen Grant Reference Mapping Bug Lets Local Users on a PV Guest System Gain Elevated Privileges on the Host System - SecurityTracker

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[500817](#) Alpine Linux Security Update for xen

[504560](#) Alpine Linux Security Update for xen

[710266](#) Gentoo Linux Xen Multiple Vulnerabilities (GLSA 201801-14)

© [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](#)