



CVE-2017-15597

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

Summary

CVE	CVE-2017-15597
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-30 14:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	An issue was discovered in Xen through 4.9.x. Grant copying code made an implication that any grant pin would be accom

Risk And Classification

Problem Types: CWE-119 | CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Xen	Xen	All	rc7	All	All

References

Reference	Source
Xen Grant Copy Race Condition Lets Local Administrative Users on a Guest System Cause the Host System to Crash - SecurityTracker	SE
Xen CVE-2017-15597 Memory Corruption Vulnerability	BI
Citrix XenServer Security Update for CVE-2017-15597	CC
[SECURITY] [DLA 1549-1] xen security update	ML
Debian -- Security Information -- DSA-4050-1 xen	DE
oss-security - Xen Security Advisory 236 (CVE-2017-15597) - pin count / page reference race in grant table code	ML
XSA-236 - Xen Security Advisories	CC
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[500820](#) Alpine Linux Security Update for xen

[504563](#) 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](#)