



CVE-2017-8903

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

Summary

CVE	CVE-2017-8903
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-05-11 19:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	Xen through 4.8.x on 64-bit platforms mishandles page tables after an IRET hypercall, which might allow PV guest OS user

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Xen	Xen	4.8.0	All	All	All
Operating System	Xen	Xen	4.8.1	All	All	All
Operating System	Xen	Xen	4.8.0	All	All	All
Operating System	Xen	Xen	4.8.1	All	All	All

References

Reference
Xen IRET Hypercall Mode Switching Bug Lets Local Users on a Guest System Gain Elevated Privileges on the Host System - SecurityTracker
Updates on XSA-213, XSA-214 and XSA-215 Xen Project Blog
Xen CVE-2017-8903 Arbitrary Code Execution Vulnerability
XSA-213 - Xen Security Advisories
Xen: Multiple vulnerabilities (GLSA 201705-11) — Gentoo security
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[500815](#) Alpine Linux Security Update for xen

[504558](#) Alpine Linux Security Update for xen

[710382](#) Gentoo Linux Xen Multiple Vulnerabilities (GLSA 201705-11)

© [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](#)