



CVE-2017-15589

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

Summary

CVE	CVE-2017-15589
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-18 08:29:00 UTC
Updated	2018-10-19 10:29:00 UTC
Description	An issue was discovered in Xen through 4.9.x allowing x86 HVM guest OS users to obtain sensitive information from the hc

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Xen	Xen	4.9.0	All	All	All
Operating System	Xen	Xen	4.9.0	All	All	All

References

Reference
XSA-239 - Xen Security Advisories
[SECURITY] [DLA 1549-1] xen security update
[SECURITY] [DLA 1181-1] xen security update
Xen: Multiple vulnerabilities (GLSA 201801-14) — Gentoo security
Debian -- Security Information -- DSA-4050-1 xen
Xen Multiple Flaws on x86 Systems Let Local Guest System Users Obtain Memory Contents and Potentially Sensitive Information, Deny Serv
Citrix XenServer Multiple Security Updates
Xen CVE-2017-15589 Information Disclosure Vulnerability
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

500819 Alpine Linux Security Update for xen

504562 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](#)