



CVE-2016-9384

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

Summary

CVE	CVE-2016-9384
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-02-22 16:59:00 UTC
Updated	2017-07-28 01:29:00 UTC
Description	Xen 4.7 allows local guest OS users to obtain sensitive host information by loading a 32-bit ELF symbol table.

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	4.7.0	All	All	All
Operating System	Xen	Xen	4.7.1	All	All	All
Operating System	Xen	Xen	4.7.0	All	All	All
Operating System	Xen	Xen	4.7.1	All	All	All

References

Reference
Xen 32-bit ELF Symbol Table Loading Error Lets Local Users on a Guest System Obtain Potentially Sensitive Information from the Host System
xenbits.xen.org/xsa/xsa194.patch
Xen: Multiple vulnerabilities (GLSA 201612-56) — Gentoo security
XSA-194 - Xen Security Advisories
Xen CVE-2016-9384 Information Disclosure Vulnerability
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy OID Mappings

Legacy CVE Mappings

500810 Alpine Linux Security Update for xen

504553 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](#)