



CVE-2016-9637

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

Summary

CVE	CVE-2016-9637
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-02-17 02:59:00 UTC
Updated	2018-02-08 02:29:00 UTC
Description	The (1) ioport_read and (2) ioport_write functions in Xen, when qemu is used as a device model within Xen, might allow loc

Risk And Classification

Problem Types: CWE-264

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	sp1	All	All
Application	Citrix	Xenserver	6.5	sp1	All	All
Application	Citrix	Xenserver	7.0	All	All	All
Application	Citrix	Xenserver	6.0.2	All	All	All
Application	Citrix	Xenserver	6.2.0	sp1	All	All
Application	Citrix	Xenserver	6.5	sp1	All	All
Application	Citrix	Xenserver	7.0	All	All	All

References

Reference
Xen ioport Array Overflow Lets Local Administrative Users on a Guest System Gain Elevated Privileges on the QEMU Process - SecurityTrack
Red Hat Customer Portal
Xen: Multiple vulnerabilities (GLSA 201612-56) — Gentoo security
XSA-199 - Xen Security Advisories
Xen CVE-2016-9637 Privilege Escalation Vulnerability
[SECURITY] [DLA 1270-1] xen security update

CVE-2016-9637 - Citrix XenServer Security Update

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#)