



CVE-2016-3157

Published on: 04/12/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:01 PM UTC

CVE-2016-3157

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

The `__switch_to` function in `arch/x86/kernel/process_64.c` in the Linux kernel does not properly context-switch IOPL on 64-bit PV Xen guests, which allows local guest OS users to gain privileges, cause a denial of service (guest OS crash), or obtain sensitive information by leveraging I/O port access.

CVE-2016-3157 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.2 - HIGH**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
USN-2969-1: Linux kernel (Utopic HWE) vulnerabilities Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2969-1
Xen I/O Port Access Missing	www.securitytracker.com	SECTrack 1035308

Xen /C P0rt Access missing PHYSDEVOP_set_iopl Hypercall Lets Local Users on a Guest System Gain Elevated Privileges on the Guest System - SecurityTracker	www.securitytracker.com text/html	SECURITYTRACKER 1000000
USN-2971-2: Linux kernel (Wily HWE) vulnerabilities Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2971-2
USN-2968-1: Linux kernel vulnerabilities Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2968-1
Oracle Linux Bulletin - April 2016	www.oracle.com text/html	CONFIRM www.oracle.com/technetwork/topics/security/linuxbulletinapr2016-2952096.html
XSA-171 - Xen Security Advisories	Patch Vendor Advisory xenbits.xen.org text/html	CONFIRM xenbits.xen.org/xsa/advisory-171.html
USN-2970-1: Linux kernel (Vivid HWE) vulnerabilities Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2970-1
USN-2968-2: Linux kernel (Trusty HWE) vulnerabilities Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2968-2
Debian -- Security Information -- DSA-3607-1 linux	www.debian.org Deprecated Link text/html	DEBIAN DSA-3607
USN-2996-1: Linux kernel vulnerabilities Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2996-1
USN-2971-1: Linux kernel vulnerabilities Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2971-1
Linux Kernel Xen PV Guest CVE-2016-3157 Local Privilege Escalation Vulnerability	cve.report (archive) text/html	BID 84594
USN-2997-1: Linux kernel (OMAP4) vulnerabilities Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2997-1
USN-2971-3: Linux kernel (Raspberry Pi 2) vulnerabilities Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2971-3

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Xen	Xen	4.0.0	All	All	All

Operating System	Xen	Xen	4.0.0	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:*:*:*:						
cpe:2.3:o:xen:xen:4.0.0:*:*:*:*:*:*:						
cpe:2.3:o:xen:xen:4.0.0:*:*:*:*:*:*:						
No vendor comments have been submitted for this CVE						
← Previous ID				Next ID→		

© [CVE.report](#) 2023   |

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](#)