

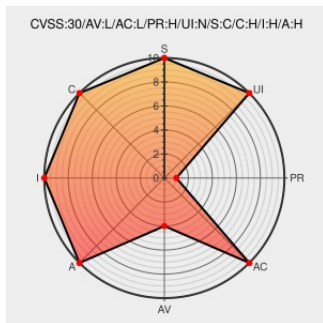


CVE-2016-7093

Published on: 09/21/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:06 PM UTC

CVE-2016-7093

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

Certain versions of [Xen](#) from [Xen](#) contain the following vulnerability:

Xen 4.5.3, 4.6.3, and 4.7.x allow local HVM guest OS administrators to overwrite hypervisor memory and consequently gain host OS privileges by leveraging mishandling of instruction pointer truncation during emulation.

CVE-2016-7093 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.2 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	HIGH	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	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
Xen: Multiple vulnerabilities (GLSA 201611-09) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-201611-09
XSA-186 - Xen Security Advisories	Patch Vendor Advisory	CONFIRM xenbits.xen.org/xsa/advisory-186.html

 SECTRAK 1036752

Xen Instruction Pointer Truncation Flaw Lets Local Users on a Guest System Gain Elevated Privileges on the Host System - SecurityTracker

Citrix XenServer Multiple Security Updates

Third Party Advisory
support.citrix.com
text/html

 CONFIRM
support.citrix.com/article/CTX216071

Patch
Vendor Advisory
xenbits.xen.org
text/x-diff

 **CONFIRM**
xenbits.xen.org/xsa/xsa186-0001-x86-
emulate-Correct-boundary-interactions-
of-emulate.patch

Xen CVE-2016-7093 Local Privilege Escalation Vulnerability

cve.report (archive)

 BID 92865

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.

Related QID Numbers

500808 Alpine Linux Security Update for xen

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Xen	Xen	4.5.3	All	All	All
Operating System	Xen	Xen	4.6.3	All	All	All
Operating System	Xen	Xen	4.7.0	All	All	All
Operating System	Xen	Xen	4.5.3	All	All	All
Operating System	Xen	Xen	4.6.3	All	All	All
Operating System	Xen	Xen	4.7.0	All	All	All
cpe:2.3:o:xen:xen:4.5.3:*:*:*:*:*:						
cpe:2.3:o:xen:xen:4.6.3:*:*:*:*:*:						
cpe:2.3:o:xen:xen:4.7.0:*:*:*:*:*:						
cpe:2.3:o:xen:xen:4.5.3:*:*:*:*:*:						
cpe:2.3:o:xen:xen:4.6.3:*:*:*:*:*:						
cpe:2.3:o:xen:xen:4.7.0:*:*:*:*:*:						

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](#)