



CVE-2014-7156

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

Summary

CVE	CVE-2014-7156
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-10-02 14:55:00 UTC
Updated	2018-10-30 16:26:00 UTC
Description	The x86_emulate function in arch/x86/x86_emulate/x86_emulate.c in Xen 3.3.x through 4.4.x does not check the superviso

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Xen	Xen	3.3.0	All	All	All
Operating System	Xen	Xen	3.3.1	All	All	All
Operating System	Xen	Xen	3.3.2	All	All	All
Operating System	Xen	Xen	4.1.0	All	All	All
Operating System	Xen	Xen	4.1.1	All	All	All
Operating System	Xen	Xen	4.1.2	All	All	All
Operating System	Xen	Xen	4.1.3	All	All	All
Operating System	Xen	Xen	4.1.4	All	All	All
Operating System	Xen	Xen	4.1.5	All	All	All
Operating System	Xen	Xen	4.1.6.1	All	All	All
Operating System	Xen	Xen	4.2.0	All	All	All
Operating System	Xen	Xen	4.2.1	All	All	All
Operating System	Xen	Xen	4.2.2	All	All	All
Operating System	Xen	Xen	4.2.3	All	All	All
Operating System	Xen	Xen	4.3.0	All	All	All
Operating System	Xen	Xen	4.3.1	All	All	All
Operating System	Xen	Xen	4.4.0	All	All	All

Operating System	Xen	Xen	4.4.0	rc1	All	All
Operating System	Xen	Xen	4.4.1	-	All	All
Operating System	Xen	Xen	3.3.0	All	All	All
Operating System	Xen	Xen	3.3.1	All	All	All
Operating System	Xen	Xen	3.3.2	All	All	All
Operating System	Xen	Xen	4.1.0	All	All	All
Operating System	Xen	Xen	4.1.1	All	All	All
Operating System	Xen	Xen	4.1.2	All	All	All
Operating System	Xen	Xen	4.1.3	All	All	All
Operating System	Xen	Xen	4.1.4	All	All	All
Operating System	Xen	Xen	4.1.5	All	All	All
Operating System	Xen	Xen	4.1.6.1	All	All	All
Operating System	Xen	Xen	4.2.0	All	All	All
Operating System	Xen	Xen	4.2.1	All	All	All
Operating System	Xen	Xen	4.2.2	All	All	All
Operating System	Xen	Xen	4.2.3	All	All	All
Operating System	Xen	Xen	4.3.0	All	All	All
Operating System	Xen	Xen	4.3.1	All	All	All
Operating System	Xen	Xen	4.4.0	All	All	All
Operating System	Xen	Xen	4.4.0	rc1	All	All
Operating System	Xen	Xen	4.4.1	-	All	All

References			
Reference	Source	Link	
[SECURITY] Fedora 20 Update: xen-4.3.3-3.fc20	FEDORA	link	
[security-announce] openSUSE-SU-2014:1279-1: important: xen: security an	SUSE	link	
Debian -- Security Information -- DSA-3041-1 xen	DEBIAN	link	
Security Advisory SA61890 - Gentoo update for xen - Secunia	SECUNIA	link	
Security Advisory SA61858 - Citrix XenServer Multiple Vulnerabilities - Secunia	SECUNIA	link	
Xen x86 Emulation Error Lets Local Guest System Users Deny Service on the Host System - SecurityTracker	SECTRAK	link	
Xen: Denial of Service (GLSA 201412-42) — Gentoo security	GENTOO	link	
Xen Supervisor Mode Permission Checks Local Denial of Service Vulnerability	BID	link	
Security Advisory SA61500 - Xen Protected Mode Software Interrupts Emulation Denial of Service Vulnerability - Secunia	SECUNIA	link	
XSA-106 - Xen Security Advisories	CONFIRM	link	
Citrix XenServer Multiple Security Updates	CONFIRM	link	
[SECURITY] Fedora 20 Update: xen-4.3.3-3.fc20	FEDORA	link	

[SECURITY] Fedora 19 Update: xen-4.2.5-3.fc19	FEDORA	IIS
[security-announce] openSUSE-SU-2014:1281-1: important: xen: security an	SUSE	IIS
CVE Program record	CVE.ORG	WV
NVD vulnerability detail	NVD	nv

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](#)