CVE-2015-0239

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2015-0239
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-03-02 11:59:04 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The em_sysenter function in arch/x86/kvm/emulate.c in the Linux kernel before 3.18.5, when the guest OS lacks SYSENTE

Risk And Classification

Primary CVSS: v2.0 4.4 from nvd@nist.gov

AV:L/AC:M/Au:N/C:P/I:P/A:P

Problem Types: CWE-269 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:L/AC:M/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All

Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Oracle	Linux	5	-	All	All
Operating System	Oracle	Linux	7	-	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
USN-2516-1: Linux kernel vulnerabilities | Ubuntu	af854a3a-2127-42
KVM: x86: SYSENTER emulation is broken · torvalds/linux@f374737 · GitHub	af854a3a-2127-42
KVM: x86: SYSENTER emulation is broken	af854a3a-2127-42
oss-security - KVM SYSENTER emulation vulnerability - CVE-2015-0239	af854a3a-2127-42
www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.18.5	af854a3a-2127-42
USN-2514-1: Linux kernel (OMAP4) vulnerabilities | Ubuntu	af854a3a-2127-42
USN-2518-1: Linux kernel vulnerabilities | Ubuntu	af854a3a-2127-42
Red Hat Customer Portal	af854a3a-2127-42
1186448 – (CVE-2015-0239) CVE-2015-0239 kernel: kvm: insufficient sysenter emulation when invoked from 16-bit code	af854a3a-2127-42
Support / Security / Advisories / / MDVSA-2015:058 | Mandriva	af854a3a-2127-42
Linux Kernel KVM CVE-2015-0239 Local Privilege Escalation Vulnerability	af854a3a-2127-42
USN-2513-1: Linux kernel vulnerabilities | Ubuntu	af854a3a-2127-42
kernel/git/torvalds/linux.git - Linux kernel source tree	af854a3a-2127-42
USN-2515-1: Linux kernel (Trusty HWE) vulnerabilities | Ubuntu	af854a3a-2127-42
Oracle Linux Bulletin - January 2016	af854a3a-2127-42
USN-2517-1: Linux kernel (Utopic HWE) vulnerabilities | Ubuntu	af854a3a-2127-42
Oracle Linux Bulletin - October 2015	af854a3a-2127-42
Debian -- Security Information -- DSA-3170-1 linux	af854a3a-2127-42
kernel/git/torvalds/linux.git - Linux kernel source tree	MITRE
Red Hat Customer Portal	MITRE

Red Hat Customer Portal	MITRE
Red Hat Customer Portal	MITRE
access.redhat.com | CVE-2015-0239	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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 registred 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**