



CVE-2017-2596

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

Summary

CVE	CVE-2017-2596
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-02-06 06:59:00 UTC
Updated	2023-02-12 23:29:00 UTC
Description	The nested_vmcheck_vmptr function in arch/x86/kvm/vmx.c in the Linux kernel through 4.9.8 improperly emulates the VM

Risk And Classification

Problem Types: CWE-772

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link	Tags
Red Hat Customer Portal	REDHAT	access.redhat.com	
Bug 1417812 – CVE-2017-2596 Kernel: kvm: page reference leakage in handle_vmon	CONFIRM	bugzilla.redhat.com	Issue Tracking
Linux Kernel CVE-2017-2596 Denial of Service Vulnerability	BID	www.securityfocus.com	Third Party A
CVE-2017-2596 - Red Hat Customer Portal	MISC	access.redhat.com	
oss-security - CVE-2017-2596 Kernel: kvm: page reference leakage in handle_vmon	MLIST	www.openwall.com	Mailing List, F
Debian -- Security Information -- DSA-3791-1 linux	DEBIAN	www.debian.org	
Red Hat Customer Portal	REDHAT	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, an

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](#)