



CVE-2014-8480

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

Summary

CVE	CVE-2014-8480
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-11-10 11:55:00 UTC
Updated	2023-11-07 02:22:00 UTC
Description	The instruction decoder in arch/x86/kvm/emulate.c in the KVM subsystem in the Linux kernel before 3.18-rc2 lacks intended

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	rc1	All	All

References

Reference	Source
thread.gmane.org 522: Connection timed out	MLIST
Bug 1156615 – CVE-2014-8480 CVE-2014-8481 kernel: kvm: NULL pointer dereference during rip relative instruction emulation	CONFIRM
oss-security - CVE Request: Linux 3.17 guest-triggerable KVM OOPS	MLIST
KVM: x86: PREFETCH and HINT_NOP should have SrcMem flag · torvalds/linux@3f6f148 · GitHub	CONFIRM
kernel/git/torvalds/linux.git - Linux kernel source tree	
Linux Kernel KVM CVE-2014-8480 Denial of Service Vulnerability	BID
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM
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 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](#)