



# CVE-2018-1087

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

## Summary

<b>CVE</b>	CVE-2018-1087
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-05-15 16:29:00 UTC
<b>Updated</b>	2019-10-09 23:38:00 UTC
<b>Description</b>	kernel KVM before versions kernel 4.16, kernel 4.16-rc7, kernel 4.17-rc1, kernel 4.17-rc2 and kernel 4.17-rc3 is vulnerable to

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Linux	Linux Kernel	4.16	All	All	All
Operating System	Linux	Linux Kernel	4.16	rc7	All	All
Operating System	Linux	Linux Kernel	4.17	rc1	All	All
Operating System	Linux	Linux Kernel	4.17	rc2	All	All
Operating System	Linux	Linux Kernel	4.17	rc3	All	All
Operating System	Linux	Linux Kernel	4.16	All	All	All
Operating System	Linux	Linux Kernel	4.16	rc7	All	All

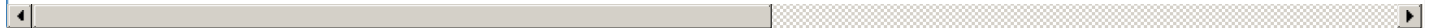
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	4.17	rc1	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	4.17	rc2	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	4.17	rc3	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	7.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	7.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	7.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	7.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	7.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	7.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Virtualization</a>	4.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Virtualization</a>	4.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All

## References

### Reference

Bug 1566837 – CVE-2018-1087 Kernel: KVM: error in exception handling leads to wrong debug stack value

Red Hat Customer Portal
POP SS debug exception - CVE-2018-8897 [Moderate] & CVE-2018-1087 [Important] - Red Hat Customer Portal
oss-security - CVE-2018-1087: KVM incorrectly handles #DB exceptions while deferred by MOV SS/POP SS
Debian -- Security Information -- DSA-4196-1 linux
Linux Kernel CVE-2018-1087 Local Privilege Escalation Vulnerability
Red Hat Customer Portal
USN-3641-2: Linux kernel vulnerabilities   Ubuntu security notices
Red Hat Customer Portal
Red Hat Customer Portal
Red Hat Customer Portal
Linux Kernel KVM Hypervisor Debug Exception Handling Flaw Lets Local Guest Users Deny Service or Gain Elevated Privileges on the Guest
USN-3641-1: Linux kernel vulnerabilities   Ubuntu security notices
Red Hat Customer Portal
CVE Program record
NVD vulnerability detail



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](#).  
**CVE.report and Source URL Uptime Status [status.cve.report](#)**