



# CVE-2019-3887

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

## Summary

<b>CVE</b>	CVE-2019-3887
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-04-09 16:29:00 UTC
<b>Updated</b>	2023-02-12 23:38:00 UTC
<b>Description</b>	A flaw was found in the way KVM hypervisor handled x2APIC Machine Specific Register (MSR) access with nested(=1) vir

## Risk And Classification

**Problem Types:** CWE-863

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.04	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	29	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.1	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Real Time</a>	8	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Real Time For Nfv</a>	8	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Real Time For Nfv Tus</a>	8.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Real Time For Nfv Tus</a>	8.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Real Time Tus</a>	8.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Real Time Tus</a>	8.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	8.2	All	All	All

Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	8.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	8.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	8.4	All	All	All

## References

Reference	Source	Link
USN-3980-1: Linux kernel vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="#">usn.ubuntu.</a>
Red Hat Customer Portal	MISC	<a href="#">access.redh</a>
[SECURITY] Fedora 29 Update: kernel-headers-5.0.7-200.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraq</a>
[SECURITY] Fedora 29 Update: kernel-headers-5.0.7-200.fc29 - package-announce - Fedora Mailing-Lists	MISC	<a href="#">lists.fedoraq</a>
USN-3980-2: Linux kernel (HWE) vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="#">usn.ubuntu.</a>
1695044 – (CVE-2019-3887) CVE-2019-3887 Kernel: KVM: nVMX: guest accesses L0 MSR causes potential DoS	MISC	<a href="#">bugzilla.red</a>
Red Hat Customer Portal	REDHAT	<a href="#">access.redh</a>
USN-3979-1: Linux kernel vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="#">usn.ubuntu.</a>
1695044 – (CVE-2019-3887) CVE-2019-3887 Kernel: KVM: nVMX: guest accesses L0 MSR causes potential DoS	CONFIRM	<a href="#">bugzilla.red</a>
Red Hat Customer Portal	REDHAT	<a href="#">access.redh</a>
Linux kernel CVE-2019-3887 Local Denial of Service Vulnerability	BID	<a href="#">www.securi</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.or</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">900101</a> CBL-Mariner Linux Security Update for kernel 5.10.52.1
<a href="#">900303</a> CBL-Mariner Linux Security Update for kernel 5.10.57.1
<a href="#">900321</a> CBL-Mariner Linux Security Update for kernel 5.10.60.1
<a href="#">901453</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6521-1)
<a href="#">903238</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3489)
<a href="#">905961</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3489-1)
<a href="#">906403</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6521-2)

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](#)**