



# CVE-2019-9003

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2019-9003
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-02-22 15:29:00 UTC
<b>Updated</b>	2021-06-02 15:31:00 UTC
<b>Description</b>	In the Linux kernel before 4.20.5, attackers can trigger a drivers/char/ipmi/ipmi_msghandler.c use-after-free and OOPS by e

## Risk And Classification

**Problem Types:** CWE-416

## 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="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.0	rc1	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.0	rc2	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.0	rc3	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.0	rc4	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">Cn1610</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">Cn1610 Firmware</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Element Software Management</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Element Software Management</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Hci Management Node</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Snapprotect</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Solidfire</a>	-	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.0	All	All	All

References				
Reference	Source	Link	Tags	
[security-announce] openSUSE-SU-2019:1404-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>		
Linux Kernel 'drivers/char/ipmi/ipmi_msghandler.c' Denial of Service Vulnerability	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>	Third Party A	
March 2019 Linux Kernel Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	Third Party A	
USN-3930-1: Linux kernel vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>		
USN-3930-2: Linux kernel (HWE) vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>		
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	<a href="https://git.kernel.org">git.kernel.org</a>	Patch, Third	
ipmi: fix use-after-free of user->release_barrier.rda · torvalds/linux@77f8269 · GitHub	MISC	<a href="https://github.com">github.com</a>	Patch, Third	
cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.20.5	MISC	<a href="https://cdn.kernel.org">cdn.kernel.org</a>	Release Note	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical	
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, ar	

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org). This site includes MITRE data granted under the following [license](https://www.mitre.org).

**CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)**