



# CVE-2018-20836

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

## Summary

<b>CVE</b>	CVE-2018-20836
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-05-07 14:29:00 UTC
<b>Updated</b>	2022-11-03 02:22:00 UTC
<b>Description</b>	An issue was discovered in the Linux kernel before 4.20. There is a race condition in smp_task_timedout() and smp_task_c

## Risk And Classification

**Problem Types:** CWE-362 | CWE-416

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	F5	Traffix Signaling Delivery Controller	5.0.0	All	All	All
Application	F5	Traffix Signaling Delivery Controller	5.1.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Application	Netapp	Active Iq Unified Manager	All	All	All	All
Hardware	Netapp	Hci Compute Node	-	All	All	All
Application	Netapp	Snapprotect	-	All	All	All
Application	Netapp	Solidfire Hci Management Node	-	All	All	All
Application	Netapp	Solidfire Hci Storage Node	-	All	All	All
Application	Netapp	Storage Replication Adapter For Clustered Data Ontap	-	All	All	All
Application	Netapp	Vasa Provider For Clustered Data Ontap	All	All	All	All
Application	Netapp	Virtual Storage Console	All	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All

Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All
------------------	--------------------------	----------------------	------	-----	-----	-----

## References

Reference	Source	Link	Tags
scsi: libsas: fix a race condition when smp task timeout · torvalds/linux@b90cd6f · GitHub	MISC	<a href="#">github.com</a>	Patch, Ve
Debian -- Security Information -- DSA-4495-1 linux	DEBIAN	<a href="#">www.debian.org</a>	
support.f5.com/csp/article/K11225249	CONFIRM	<a href="#">support.f5.com</a>	
Debian -- Security Information -- DSA-4497-1 linux	DEBIAN	<a href="#">www.debian.org</a>	
[security-announce] openSUSE-SU-2019:1716-1: important: Security update	SUSE	<a href="#">lists.opensuse.org</a>	
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	<a href="#">git.kernel.org</a>	Patch, Ve
Bugtraq: [SECURITY] [DSA 4495-1] linux security update	BUGTRAQ	<a href="#">seclists.org</a>	
USN-4076-1: Linux kernel vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="#">usn.ubuntu.com</a>	
[security-announce] openSUSE-SU-2019:1757-1: important: Security update	SUSE	<a href="#">lists.opensuse.org</a>	
Linux Kernel CVE-2018-20836 Race Condition Vulnerability	BID	<a href="#">www.securityfocus.com</a>	
May 2019 Linux Kernel Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="#">security.netapp.com</a>	
Bugtraq: [SECURITY] [DSA 4497-1] linux security update	BUGTRAQ	<a href="#">seclists.org</a>	
[SECURITY] [DLA 1884-1] linux security update	MLIST	<a href="#">lists.debian.org</a>	
[SECURITY] [DLA 1885-1] linux-4.9 security update	MLIST	<a href="#">lists.debian.org</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical

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](#)