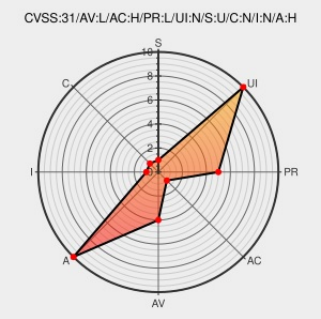
CVE-2019-19065

Published on: 11/18/2019 12:00:00 AM UTC

Last Modified on: 11/07/2023 03:07:00 AM UTC

CVE-2019-19065

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

** DISPUTED ** A memory leak in the sdma_init() function in drivers/infiniband/hw/hfi1/sdma.c in the Linux kernel before 5.3.9 allows attackers to cause a denial of service (memory consumption) by triggering rhashtable_init() failures, aka CID-34b3be18a04e. NOTE: This has been disputed as not a vulnerability because "rhashtable_init() can only fail if it is passed invalid values in the second parameter's struct, but when invoked from sdma_init() that is a pointer to a static const struct, so an attacker could only trigger failure if they could corrupt kernel memory (in which case a small memory leak is not a significant problem)."

CVE-2019-19065 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 4.7 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	HIGH	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 4.7 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
November 2019 Linux Kernel Vulnerabilities in NetApp Products | NetApp Product Security	Third Party Advisory security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20191205-0001/
RDMA/hfi1: Prevent memory leak in sdma_init · torvalds/linux@34b3be1 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/torvalds/linux/commit/34b3be18a04ecdc610aae4c48e5d1b799d8689f6
USN-4226-1: Linux kernel vulnerabilities | Ubuntu security notices | Ubuntu	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-4226-1
USN-4210-1: Linux kernel vulnerabilities | Ubuntu security notices | Ubuntu	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-4210-1
[security-announce] openSUSE-SU-2019:2675-1: important: Security update	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2019:2675
	Release Notes Vendor Advisory cdn.kernel.org text/plain	MISC cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.3.9
USN-4208-1: Linux kernel vulnerabilities | Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-4208-1

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All

Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:19.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:19.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:19.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:19.10:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:15.1:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:15.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→