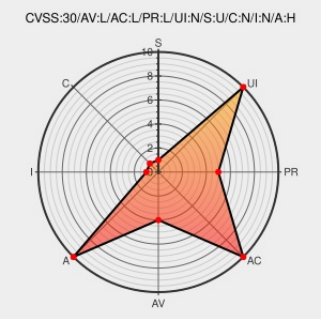
CVE-2018-10021

Published on: 04/11/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:21 PM UTC

CVE-2018-10021

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



Certain versions of Linux Kernel from Linux contain the following vulnerability:

** DISPUTED ** drivers/scsi/libsas/sas_scsi_host.c in the Linux kernel before 4.16 allows local users to cause a denial of service (ata qc leak) by triggering certain failure conditions. NOTE: a third party disputes the relevance of this report because the failure can only occur for physically proximate attackers who unplug SAS Host Bus Adapter cables.

CVE-2018-10021 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.5 - MEDIUM

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

CVSS2 Score: 4.9 - MEDIUM

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

CVE References

Description	Tags	Link
USN-3678-1: Linux kernel vulnerabilities | Ubuntu security	usn.ubuntu.com text/html	UBUNTU USN-3678-1

notices		
USN-3696-2: Linux kernel (Xenial HWE) vulnerabilities | Ubuntu security notices	usn.ubuntu.com text/html	UBUNTU USN-3696-2
USN-3678-2: Linux kernel (Azure) vulnerabilities | Ubuntu security notices | Ubuntu	usn.ubuntu.com text/html	UBUNTU USN-3678-2
USN-3696-1: Linux kernel vulnerabilities | Ubuntu security notices	usn.ubuntu.com text/html	UBUNTU USN-3696-1
USN-3678-4: Linux kernel (Raspberry Pi 2) vulnerabilities | Ubuntu security notices | Ubuntu	usn.ubuntu.com text/html	UBUNTU USN-3678-4
[SECURITY] [DLA 1423-1] linux-4.9 new package	lists.debian.org text/html	MLIST [debian-lts-announce] 20180718 [SECURITY] [DLA 1423-1] linux-4.9 new package
kernel/git/torvalds/linux.git - Linux kernel source tree	Vendor Advisory git.kernel.org text/html	MISC git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=318aaf34f1179b39fa9c30fa0f3288b645beee39
scsi: libsas: defer ata device eh commands to libata · torvalds/linux@318aaf3 · GitHub	Third Party Advisory github.com text/html	MISC github.com/torvalds/linux/commit/318aaf34f1179b39fa9c30fa0f3288b645beee39
USN-3754-1: Linux kernel vulnerabilities | Ubuntu security notices | Ubuntu	usn.ubuntu.com text/html	UBUNTU USN-3754-1
USN-3678-3: Linux kernel (Azure) vulnerabilities | Ubuntu security notices | Ubuntu	usn.ubuntu.com text/html	UBUNTU USN-3678-3
Bug 1089281 – VUL-0: CVE-2018-10021: kernel-source: drivers/scsi/libsas/sas_scsi_host.c in the Linux kernel before 4.16 allows localusers to cause a denial of service (ata qc leak) by triggering certain failureconditions.	Issue Tracking Third Party Advisory bugzilla.suse.com text/html	MISC bugzilla.suse.com/show_bug.cgi?id=1089281

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→