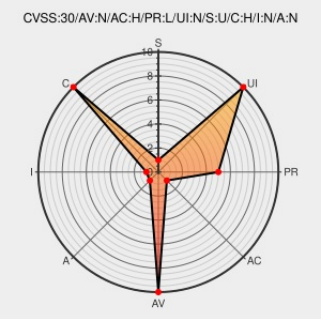
CVE-2018-1000204

Published on: 06/26/2018 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:51:00 AM UTC

CVE-2018-1000204

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



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

** DISPUTED ** Linux Kernel version 3.18 to 4.16 incorrectly handles an SG_IO ioctl on /dev/sg0 with dxfer_direction=SG_DXFER_FROM_DEV and an empty 6-byte cmdp. This may lead to copying up to 1000 kernel heap pages to the userspace. This has been fixed upstream in https://github.com/torvalds/linux/commit/a45b599ad808c3c982fdcdc12b0b8611c2f92824 already. The problem has limited scope, as users don't usually have permissions to access SCSI devices. On the other hand, e.g. the Nero user manual suggests doing `chmod o+r+w /dev/sg*` to make the devices accessible. NOTE: third parties dispute the relevance of this report, noting that the requirement for an attacker to have both the CAP_SYS_ADMIN and CAP_SYS_RAWIO capabilities makes it "virtually impossible to exploit."

CVE-2018-1000204 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.3 - MEDIUM

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

CVSS2 Score: 6.3 - MEDIUM

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

CVE References

Description	Tags	Link
[security-announce] openSUSE-SU-2019:1407-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2019:1407
USN-3696-2: Linux kernel (Xenial HWE) vulnerabilities | Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3696-2
USN-3752-1: Linux kernel vulnerabilities | Ubuntu security notices | Ubuntu	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3752-1
USN-3752-2: Linux kernel (HWE) vulnerabilities | Ubuntu security notices | Ubuntu	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3752-2
USN-3696-1: Linux kernel vulnerabilities | Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3696-1
oss-security - Re: CVE-2018-1000204: Linux kernel 3.18 to 4.16 infoleak due to incorrect handling of SG_IO ioctl	Mailing List Third Party Advisory www.openwall.com text/html	MISC www.openwall.com/lists/oss-security/2018/06/26/3
[SECURITY] [DLA 1422-1] linux security update	Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20180714 [SECURITY] [DLA 1422-1] linux security update
[SECURITY] [DLA 1423-1] linux-4.9 new package	Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20180718 [SECURITY] [DLA 1423-1] linux-4.9 new package
[SECURITY] [DLA 1422-2] linux security update	Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20180715 [SECURITY] [DLA 1422-2] linux security update
scsi: sg: allocate with __GFP_ZERO in sg_build_indirect() · torvalds/linux@a45b599 · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/torvalds/linux/commit/a45b599ad808c3c982fdcdc12b0b8611c2f92824
USN-3752-3: Linux kernel (Azure, GCP, OEM) vulnerabilities | Ubuntu security notices | Ubuntu	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3752-3
USN-3754-1: Linux kernel vulnerabilities | Ubuntu security notices | Ubuntu	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3754-1
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2018:2948

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	14.04	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	14.04	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	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

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:14.04:*:*:*:lts:*:*:*:

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

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

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report