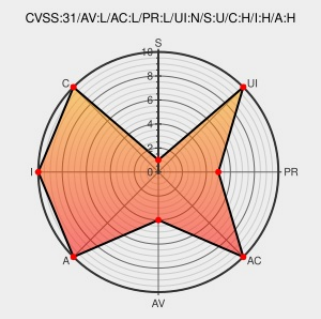
CVE-2018-10878

Published on: 07/26/2018 12:00:00 AM UTC

Last Modified on: 10/05/2023 02:15:00 PM UTC

CVE-2018-10878

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



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

A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause an out-of-bounds write and a denial of service or unspecified other impact is possible by mounting and operating a crafted ext4 filesystem image.

CVE-2018-10878 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **[UNKNOWN]** - **kernel** version **= n/a**

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 6.1 - MEDIUM

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

CVE References

Description	Tags	Link
1596802 – (CVE-2018-10878) CVE-2018-10878 kernel: out-of-bound write in ext4_init_block_bitmap function with a crafted ext4	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1596802

image		
USN-3871-3: Linux kernel (AWS, GCP, KVM, OEM, Raspberry Pi 2) vulnerabilities | Ubuntu security notices | Ubuntu	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3871-3
[SECURITY] [DLA 1423-1] linux-4.9 new package	Mailing List Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20180718 [SECURITY] [DLA 1423-1] linux-4.9 new package
1596802 – (CVE-2018-10878) CVE-2018-10878 kernel: out-of-bound write in ext4_init_block_bitmap function with a crafted ext4 image	Issue Tracking Patch bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-10878
kernel/git/torvalds/linux.git - Linux kernel source tree	Patch Vendor Advisory git.kernel.org text/html	CONFIRM git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=77260807d1170a8cf35dbb06e07461a655f67eee
USN-3871-5: Linux kernel (Azure) vulnerabilities | Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3871-5
CVE-2018-10878 - Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2018-10878
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2018:3083
USN-3871-4: Linux kernel (HWE) vulnerabilities | Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3871-4
199865 – out-of-bound write in ext4_init_block_bitmap() when mounting and operating a crafted ext4 image	Exploit Issue Tracking Patch Vendor Advisory bugzilla.kernel.org text/html	CONFIRM bugzilla.kernel.org/show_bug.cgi?id=199865
kernel/git/torvalds/linux.git - Linux kernel source tree	Patch Vendor Advisory git.kernel.org text/html	CONFIRM git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=819b23f1c501b17b9694325471789e6b5cc2d0d2
[2/3] ext4: make sure bitmaps and the inode table don't overlap with bg descriptors - Patchwork	Patch Third Party Advisory patchwork.ozlabs.org text/html	CONFIRM patchwork.ozlabs.org/patch/929238/
USN-3753-1: Linux kernel vulnerabilities | Ubuntu security notices | Ubuntu	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3753-1
USN-3871-1: Linux kernel vulnerabilities | Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3871-1
USN-3753-2: Linux kernel (Xenial HWE) vulnerabilities | Ubuntu security notices | Ubuntu	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3753-2
Red Hat Customer Portal	Third Party Advisory access.redhat.com	REDHAT RHSA-2018:2948

	text/html	
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2018:3096
[1/3] ext4: always check block group bounds in ext4_init_block_bitmap() - Patchwork	Patch Third Party Advisory patchwork.ozlabs.org text/html	CONFIRM patchwork.ozlabs.org/patch/929237/

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
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating	Redhat	Enterprise Linux Workstation	7.0	All	All	All

System						
Operating System	Redhat	Enterprise Linux Workstation	7.0	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:*:*:*:*:*:*:*:*
cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*
cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:*:*:*:*:*:*:*
cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:*:*:*:*:*:*:*
cpe:2.3:o:redhat:enterprise_linux_server:7.0:*:*:*:*:*:*:*
cpe:2.3:o:redhat:enterprise_linux_server:7.0:*:*:*:*:*:*:*
cpe:2.3:o:redhat:enterprise_linux_workstation:7.0:*:*:*:*:*:*:*
cpe:2.3:o:redhat:enterprise_linux_workstation:7.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→