



CVE-2018-10879

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2018-10879 |
| State | PUBLIC |
| Assigner | secalert@redhat.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2018-07-26 18:29:00 UTC |
| Updated | 2023-02-13 04:51:00 UTC |
| Description | A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause a use-after-free in ext4_xattr_set_entry functi |

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

| 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 | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 7.0 | 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 System | Redhat | Enterprise Linux Workstation | 7.0 | All | All | All |

| | | | | | | |
|------------------|--------|------------------------------|-----|-----|-----|-----|
| Operating System | Redhat | Enterprise Linux Workstation | 7.0 | All | All | All |
|------------------|--------|------------------------------|-----|-----|-----|-----|

References

| Reference | Source | Link |
|---|---------|-------------------------|
| USN-3871-3: Linux kernel (AWS, GCP, KVM, OEM, Raspberry Pi 2) vulnerabilities Ubuntu security notices Ubuntu | UBUNTU | usn.u |
| 1596806 – (CVE-2018-10879) CVE-2018-10879 kernel: use-after-free detected in ext4_xattr_set_entry with a crafted file | MISC | bugz |
| 200001 – use-after-free detected by KASAN in ext4_xattr_set_entry when renaming a file in a crafted ext4 image | CONFIRM | bugz |
| [2/2] ext4: always verify the magic number in xattr blocks - Patchwork | CONFIRM | patch |
| [SECURITY] [DLA 1423-1] linux-4.9 new package | MLIST | lists.c |
| Linux Kernel CVE-2018-10879 Local Denial of Service Vulnerability | BID | www |
| USN-3871-5: Linux kernel (Azure) vulnerabilities Ubuntu security notices | UBUNTU | usn.u |
| [1/2] ext4: add corruption check in ext4_xattr_set_entry() - Patchwork | CONFIRM | patch |
| Red Hat Customer Portal | REDHAT | acce: |
| 1596806 – (CVE-2018-10879) CVE-2018-10879 kernel: use-after-free detected in ext4_xattr_set_entry with a crafted file | CONFIRM | bugz |
| kernel/git/torvalds/linux.git - Linux kernel source tree | CONFIRM | git.ke |
| USN-3871-4: Linux kernel (HWE) vulnerabilities Ubuntu security notices | UBUNTU | usn.u |
| CVE-2018-10879 - Red Hat Customer Portal | MISC | acce: |
| USN-3753-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu | UBUNTU | usn.u |
| USN-3871-1: Linux kernel vulnerabilities Ubuntu security notices | UBUNTU | usn.u |
| USN-3753-2: Linux kernel (Xenial HWE) vulnerabilities Ubuntu security notices Ubuntu | UBUNTU | usn.u |
| kernel/git/torvalds/linux.git - Linux kernel source tree | CONFIRM | git.ke |
| Red Hat Customer Portal | REDHAT | acce: |
| Red Hat Customer Portal | REDHAT | acce: |
| CVE Program record | CVE.ORG | www |
| NVD vulnerability detail | NVD | nvd.r |

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