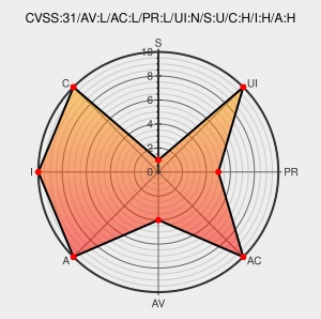
# CVE-2018-6954

Published on: 02/13/2018 12:00:00 AM UTC

Last Modified on: 01/31/2022 06:25:00 PM UTC

## CVE-2018-6954

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




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

systemd-tmpfiles in systemd through 237 mishandles symlinks present in non-terminal path components, which allows local users to obtain ownership of arbitrary files via vectors involving creation of a directory and a file under that directory, and later replacing that directory with a symlink. This occurs even if the fs.protected_symlinks sysctl is turned on.

CVE-2018-6954 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

### 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: 7.2 - HIGH

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

### CVE References

| Description | Tags | Link |
|---|---|---|
| Pony Mail! | lists.apache.org<br>text/html | MLIST [bookkeeper-issues] 20210629 [GitHub] [bookkeeper] padma81 opened a new issue #2746: Security |

| | | |
|---|---|---|
| | | Vulnerabilities in CentOS 7 image, Upgrade image to CentOS 8 |
| USN-3816-1: systemd vulnerabilities \| Ubuntu security notices \| Ubuntu | Third Party Advisory<br>usn.ubuntu.com<br>text/html | UBUNTU USN-3816-1 |
| USN-3816-2: systemd vulnerability \| Ubuntu security notices | Third Party Advisory<br>usn.ubuntu.com<br>text/html | UBUNTU USN-3816-2 |
| [security-announce] openSUSE-SU-2019:1450-1: important: Security update | lists.opensuse.org<br>text/html | SUSE openSUSE-SU-2019:1450 |
| Pony Mail! | lists.apache.org<br>text/html | MLIST [bookkeeper-issues] 20210628 [GitHub] [bookkeeper] padma81 opened a new issue #2746: Security Vulnerabilities in CentOS 7 image, Upgrade image to CentOS 8 |
| tmpfiles: symlinks are followed in non-terminal path components (CVE-2018-6954) · Issue #7986 · systemd/systemd · GitHub | Exploit<br>Patch<br>Third Party Advisory<br>github.com<br>text/html | MISC github.com/systemd/systemd/issues/7986 |



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 | 18.10 | 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 | 18.10 | All | All | All |
| Application | Freedesktop | Systemd | All | All | All | All |
| Operating System | Opensuse | Leap | 42.3 | All | All | All |
| Application | Systemd Project | Systemd | All | 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:18.10:*:*:*:*:*:*:*:

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:18.10:*:*:*:*:*:*:*:

cpe:2.3:a:freedesktop:systemd:*:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:42.3:*:*:*:*:*:*:*:

cpe:2.3:a:systemd_project:systemd:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→