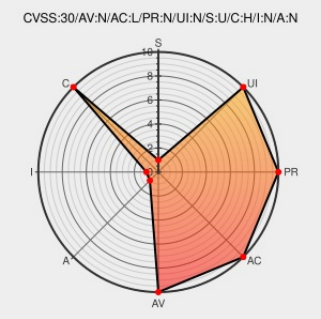
# CVE-2019-13179

Published on: 07/02/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:45 PM UTC

## CVE-2019-13179

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




Certain versions of Calamares from Calamares contain the following vulnerability:

Calamares versions 3.1 through 3.2.10 copies a LUKS encryption keyfile from /crypto_keyfile.bin (mode 0600 owned by root) to /boot within a globally readable initramfs image with insecure permissions, which allows this originally protected file to be read by any user, thereby disclosing decryption keys for LUKS containers created with Full Disk Encryption.

CVE-2019-13179 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

### CVSS3 Score: 7.5 - HIGH

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

### CVSS2 Score: 5 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| PARTIAL | NONE | NONE |

### CVE References

| Description | Tags | Link |
|---|---|---|
| Bug #1835095 “Lubuntu initrd images leaking cryptographic secret...” : Bugs : calamares package : Ubuntu | Exploit, Issue Tracking | MISC bugs.launchpad.net/ubuntu/+source/initramfs- |

| | | |
|---|---|---|
| | Third Party Advisory<br>bugs.launchpad.net<br>text/html | tools/+bug/1835095 |
| [SECURITY] Fedora 29 Update: calamares-3.2.11-1.fc29 - package-announce - Fedora Mailing-Lists | lists.fedoraproject.org<br>text/html | FEDORA FEDORA-2019-e61a85c2bb |
| [SECURITY] Fedora 30 Update: calamares-3.2.11-1.fc30 - package-announce - Fedora Mailing-Lists | lists.fedoraproject.org<br>text/html | FEDORA FEDORA-2019-50ee491d76 |
| Calamares Initramfs Weakness – Calamares – The universal installer framework | Vendor Advisory<br>calamares.io<br>text/html | CONFIRM calamares.io/calamares-cve-2019/ |
| 1726542 – (CVE-2019-13179) CVE-2019-13179 calamares: incorrect permission leads to disclosure of decryption keys for LUKS container | Issue Tracking<br>Third Party Advisory<br>bugzilla.redhat.com<br>text/html | MISC bugzilla.redhat.com/show_bug.cgi?id=1726542 |
| Bug #1835096 “Unprivileged user can access LUKS keyfile” : Bugs : initramfs-tools package : Ubuntu | Third Party Advisory<br>bugs.launchpad.net<br>text/html | MISC bugs.launchpad.net/ubuntu/+source/initramfs-tools/+bug/1835096 |
| Unsafe generation of initramfs during FDE · Issue #1191 · calamares/calamares · GitHub | Exploit<br>Issue Tracking<br>Third Party Advisory<br>github.com<br>text/html | MISC github.com/calamares/calamares/issues/1191 |
| Calamares 3.2.11 released - Calamares | Vendor Advisory<br>calamares.io<br>text/html | CONFIRM calamares.io/calamares-3.2.11-is-out/ |



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Calamares | Calamares | All | All | All | All |

cpe:2.3:a:calamares:calamares:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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