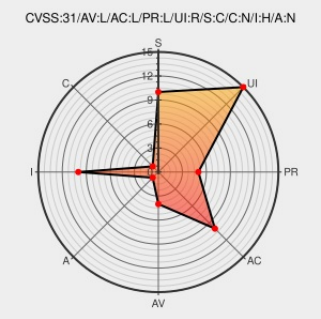
CVE-2020-11934

Published on: 07/29/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:24 PM UTC

CVE-2020-11934 - advisory for https://ubuntu.com/USN-4424-1

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



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

It was discovered that snapctl user-open allowed altering the $XDG_DATA_DIRS environment variable when calling the system xdg-open. OpenURL() in usersession/userd/launcher.go would alter $XDG_DATA_DIRS to append a path to a directory controlled by the calling snap. A malicious snap could exploit this to bypass intended access restrictions to control how the host system xdg-open script opens the URL and, for example, execute a script shipped with the snap without confinement. This issue did not affect Ubuntu Core systems. Fixed in snapd versions 2.45.1ubuntu0.2, 2.45.1+18.04.2 and 2.45.1+20.04.2.

CVE-2020-11934 has been assigned by security@ubuntu.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Canonical** - **snapd** version **< 2.45.1ubuntu0.2**

Affected Vendor/Software: **Canonical** - **snapd** version **< 2.45.1+18.04.2**

Affected Vendor/Software: **Canonical** - **snapd** version **< 2.45.1+20.04.2**

CVSS3 Score: 5.9 - MEDIUM

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

CVSS2 Score: 1.9 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
USN-4424-1: snapd vulnerabilities | Ubuntu security notices | Ubuntu	Vendor Advisory ubuntu.com text/html	CONFIRM ubuntu.com/USN-4424-1
Bug #1880085 “snap userd's OpenURL method allows sandox escape” : Bugs : snapd	Third Party Advisory launchpad.net text/html	CONFIRM launchpad.net/bugs/1880085

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	19.10	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	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	19.10	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	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:19.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:20.04:*:*:*: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:19.10:*:*:*:*:*:*:*

cpe:2.3:o:canonical:ubuntu_linux:20.04:*:*:*:lts:*:*:*

Discovery Credit

James Henstridge

← Previous ID

Next ID→