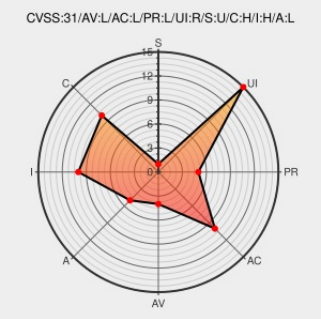
CVE-2020-27348

Published on: 12/03/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:29 PM UTC

CVE-2020-27348 - advisory for https://usn.ubuntu.com/usn/usn-4661-1

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



Certain versions of Snapcraft from Canonical contain the following vulnerability:

In some conditions, a snap package built by snapcraft includes the current directory in LD_LIBRARY_PATH, allowing a malicious snap to gain code execution within the context of another snap if both plug the home interface or similar. This issue affects snapcraft versions prior to 4.4.4, prior to 2.43.1+16.04.1, and prior to 2.43.1+18.04.1.

CVE-2020-27348 has been assigned by security@ubuntu.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Canonical** - **snapcraft** version **< 4.4.4**

Affected Vendor/Software: **Canonical** - **snapcraft** version **< 2.43.1+16.04.1**

Affected Vendor/Software: **Canonical** - **snapcraft** version **< 2.43.1+18.04.1**

CVSS3 Score: 6.8 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	LOW

CVSS2 Score: 4.4 - MEDIUM

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

CVE References

Description	Tags	Link
USN-4661-1: Snapcraft vulnerability | Ubuntu security notices | Ubuntu	Patch Third Party Advisory usn.ubuntu.com text/html	MISC usn.ubuntu.com/usn/usn-4661-1
Bug #1901572 “snapd vulnerable to Library Injection from CWD” : Bugs : Snapcraft	Exploit Issue Tracking Third Party Advisory bugs.launchpad.net text/html	MISC bugs.launchpad.net/bugs/1901572
project_loader, formatting_utils: take empty env values into account by sergiusens · Pull Request #3345 · snapcore/snapcraft · GitHub	Third Party Advisory github.com text/html	MISC github.com/snapcore/snapcraft/pull/3345

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Canonical	Snapcraft	All	All	All	All
Application	Canonical	Snapcraft	All	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	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All

cpe:2.3:a:canonical:snapcraft:*:*:*:*:*:*:*:*:

cpe:2.3:a:canonical:snapcraft:*:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:*:*:*:*:

Discovery Credit

itszn

Social Mentions

Source	Title	Posted (UTC)
@ret2systems	Snapcraft Packages Come With Extra Baggage: Exploiting Ubuntu's Snapcraft Apps with CVE-2020-27348… twitter.com/i/web/status/1…	2021-08-04 15:30:14
@_r_netsec	Ubuntu's Snapcraft Packages Come With Extra Baggage: CVE-2020-27348 blog.ret2.io/2021/08/04/sna…	2021-08-04 15:43:06
@Myinfosecfeed	New post: "Ubuntu's Snapcraft Packages Come With Extra Baggage: CVE-2020-27348" ift.tt/3ypDGF7	2021-08-04 15:48:23
@CybrXx0	Ubuntu's Snapcraft Packages Come With Extra Baggage: CVE-2020-27348 via /r/netsec ift.tt/3rX1ii2 #cybersecurity #netsec #news	2021-08-04 15:59:52
@ipssignatures	I know no IPS that has a protection/signature/rule for the vulnerability CVE-2020-27348. The vuln was published 243… twitter.com/i/web/status/1…	2021-08-04 17:04:01
@ipssignatures	The vuln CVE-2020-27348 has a tweet created 0 days ago and retweeted 15 times. twitter.com/ret2systems/st… #Snbzxv5xtl6wf4	2021-08-04 17:04:01
@axcheron	Snapcraft Packages Come With Extra Baggage - Exploiting Ubuntu's Snapcraft Apps with CVE-2020-27348… twitter.com/i/web/status/1…	2021-08-04 17:05:33
@1nf0s3cpt	Exploiting Ubuntu's Snapcraft Apps with CVE-2020-27348 blog.ret2.io/2021/08/04/sna…	2021-08-05 01:06:28
@WilfridBlanc	Ubuntu's Snapcraft Packages Come With Extra Baggage: #CVE-2020-27348 blog.ret2.io/2021/08/04/sna…	2021-08-05 06:00:03
@KeoXes	Ubuntu's Snapcraft Packages Come With Extra Baggage: CVE-2020-27348: ift.tt/3ypDGF7 #follow & #RT #cybersecurity #infosec	2021-08-05 07:33:11
@techadversary	Ubuntu's Snapcraft Packages Come With Extra Baggage: CVE-2020-27348 reddit.com/r/netsec/comme… https://t.co/3csyMR3pQN	2021-08-09 17:53:03
/r/netsec	Ubuntu's Snapcraft Packages Come With Extra Baggage: CVE-2020-27348	2021-08-04 15:32:21
/r/linux	Ubuntu's Snapcraft Packages Come With Extra Baggage: CVE-2020-27348	2021-08-05 17:43:38
/r/bag_o_news	Snapcraft Packages Come With Extra Baggage - Exploiting Ubuntu's Snapcraft Apps with CVE-2020-27348	2021-08-06 11:44:15

← Previous ID

Next ID→