

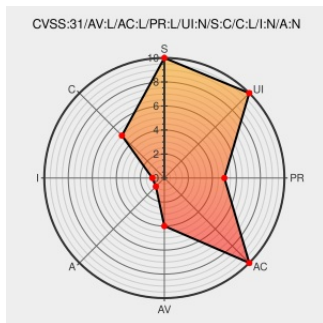


CVE-2014-1420

Published on: 09/10/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:48 PM UTC

CVE-2014-1420 - advisory for

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Ubuntu-ui-toolkit](#) from [Canonical](#) contain the following vulnerability:

On desktop, Ubuntu UI Toolkit's StateSaver would serialise data on tmp/ files which an attacker could use to expose potentially sensitive data. StateSaver would also open files without the O_EXCL flag. An attacker could exploit this to launch a symlink attack, though this is partially mitigated by symlink and hardlink restrictions in Ubuntu. Fixed in 1.1.1188+14.10.20140813.4-0ubuntu1.

CVE-2014-1420 has been assigned by security@ubuntu.com to track the vulnerability - currently rated as **LOW** severity.

Affected Vendor/Software: **Canonical** - **ubuntu-ui-toolkit** version < 1.1.1188+14.10.20140813.4-0ubuntu1

CVSS3 Score: **3.3 - LOW**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	LOW	NONE	NONE

CVSS2 Score: **2.1 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
-------------	------	------

Bug #1348241 "StateSaver serializes potentially sensitive data u..." : Bugs : Ubuntu UI Toolkit

Issue Tracking

Third Party Advisory

launchpad.net

text/html

UBUNTU

launchpad.net/bugs/1348241

~ubuntu-sdk-team/ubuntu-ui-toolkit/staging : revision 1182

Patch

Third Party Advisory

bazaar.launchpad.net

text/xml

UBUNTU

bazaar.launchpad.net/~ubuntu-sdk-team/ubuntu-ui-toolkit/staging/revision/1182

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Canonical	Ubuntu-ui-toolkit	All	All	All	All
Application	Canonical	Ubuntu-ui-toolkit	All	All	All	All

cpe:2.3:a:canonical:ubuntu-ui-toolkit:*:*:*:*:*:

cpe:2.3:a:canonical:ubuntu-ui-toolkit:*:*:*:*:*:

Discovery Credit

Olivier Tilloy

← Previous ID

Next ID →