

Your submission was sent successfully! [Close](#)

Thank you for contacting us. A member of our team will be in touch shortly. [Close](#)

You have successfully unsubscribed! [Close](#)

Thank you for signing up for our newsletter!

In these regular emails you will find the latest updates about Ubuntu and upcoming events where you can meet our team. [Close](#)

Your preferences have been successfully updated. [Close notification](#)

Please try again or [file a bug report. <https://github.com/canonical/ubuntu.com/issues/new?template=ISSUE_TEMPLATE.yaml>](https://github.com/canonical/ubuntu.com/issues/new?template=ISSUE_TEMPLATE.yaml) [Close](#)

1. [Ubuntu Security Notices](#)
2. USN-3598-2

USN-3598-2: curl vulnerabilities

Publication date

24 May 2018

Overview

Several security issues were fixed in curl.

Releases

[12.04](#)

Open side navigation

We use cookies and similar methods to recognize visitors and remember preferences. We also use them to measure campaign effectiveness and analyze traffic on our websites. By selecting 'Accept', you consent to the use of these methods by us and trusted third parties. For further details or to change your consent choices at any time see our [cookie policy <https://canonical.com/legal/data-privacy?cp=hide#cookies>](https://canonical.com/legal/data-privacy?cp=hide#cookies) .

[Manage your tracker settings](#)

Accept all

Original advisory details:

Phan Thanh discovered that curl incorrectly handled certain FTP paths. An attacker could use this to cause a denial of service or possibly execute arbitrary code. ([CVE-2018-1000120](#))

Dario Weisser discovered that curl incorrectly handled certain LDAP URLs. An attacker could possibly use this issue to cause a denial of service. ([CVE-2018-1000121](#))

Max Dymond discovered that curl incorrectly handled certain RTSP data. An attacker could possibly use this to cause a denial of service or even to get access to sensitive data. ([CVE-2018-1000122](#))

Max Dymond discovered that curl incorrectly handled certain RTSP responses. If a user or automated system were...

Show more

Update instructions

In general, a standard system update will make all the necessary changes.

[Learn more about how to get the fixes.](#)

The problem can be corrected by updating your system to the following package versions:

Ubuntu Release	Package Version
12.04 precise	libcurl3-nss < https://launchpad.net/ubuntu/+source/curl > – 7.22.0-3ubuntu4.21 < https://launchpad.net/ubuntu/+source/curl/7.22.0-3ubuntu4.21 >

We use cookies and similar methods to recognize visitors and remember preferences. We also use them to measure campaign effectiveness and analyze traffic on our websites. By selecting 'Accept', you consent to the use of these methods by us and trusted third parties. For further details or to change your consent choices at any time see our [cookie policy](#) <<https://canonical.com/legal/data-privacy?cp=hide#cookies>> .

Ubuntu Release	Package Version
	libcurl3 < https://launchpad.net/ubuntu/+source/curl > – 7.22.0-3ubuntu4.21 < https://launchpad.net/ubuntu/+source/curl/7.22.0-3ubuntu4.21 >

Reduce your security exposure

Ubuntu Pro provides ten-year security coverage to 25,000+ packages in Main and Universe repositories, and it is free for up to five machines.

[Get Ubuntu Pro](#)

References

- [CVE-2018-1000301](#)
- [CVE-2018-1000122](#)
- [CVE-2018-1000121](#)
- [CVE-2018-1000120](#)

Related notices

- [USN-3648-1](#)
- [USN-3598-1](#)

Have additional questions?

[Talk to a member of the team](#) › <https://wiki.ubuntu.com/SecurityTeam/FAQ?_ga=2.242131138.1744859116.1742138161-1500419473.1726851136&_gl=1*161muja*_gcl_au*MzUyMTIzNjI1LjE3MzYyNDQ4NTE.#Contact>

We use cookies and similar methods to recognize visitors and remember preferences. We also use them to measure campaign effectiveness and analyze traffic on our websites. By selecting 'Accept', you consent to the use of these methods by us and trusted third parties. For further details or to change your consent choices at any time see our [cookie policy](#) <<https://canonical.com/legal/data-privacy?cp=hide#cookies>> .