

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-3882-1

USN-3882-1: curl vulnerabilities

Publication date

6 February 2019

Overview

Several security issues were fixed in curl.

Releases

[18.10](#) [18.04 LTS](#) [16.04 LTS](#) [14.04 LTS](#)

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

applied to Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, and Ubuntu 18.10.

([CVE-2018-16890](#))

Wenxiang Qian discovered that curl incorrectly handled certain NTLMv2 authentication messages. A remote attacker could use this issue to cause curl to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only applied to Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, and Ubuntu 18.10. ([CVE-2019-3822](#))

Brian Carpenter discovered that curl incorrectly handled certain SMTP responses. A remote attacker could possibly use this issue to cause curl to crash, resulting in a denial of service. ([CVE-2019-3823](#))

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
18.10 cosmic	curl < https://launchpad.net/ubuntu/+source/curl > – 7.61.0-1ubuntu2.3 7.61.0-1ubuntu2.3
	libcurl3-gnutls 7.61.0-1ubuntu2.3 – 7.61.0-1ubuntu2.3

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
	7.61.0-1ubuntu2.3
	curl 7.58.0-2ubuntu3.6
	7.58.0-2ubuntu3.6
	libcurl3-gnutls 7.58.0-2ubuntu3.6
	7.58.0-2ubuntu3.6
18.04 LTS bionic	libcurl3-nss 7.58.0-2ubuntu3.6
	7.58.0-2ubuntu3.6
	libcurl4 7.58.0-2ubuntu3.6
	7.58.0-2ubuntu3.6
16.04 LTS xenial	curl 7.47.0-1ubuntu2.12
	7.47.0-1ubuntu2.12
	libcurl3 7.47.0-1ubuntu2.12
	7.47.0-1ubuntu2.12

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>](https://canonical.com/legal/data-privacy?cp=hide#cookies) .

Ubuntu Release	Package Version
	7.47.0-1ubuntu2.12
	curl 7.35.0-1ubuntu2.20
	7.35.0-1ubuntu2.20
	libcurl3 7.35.0-1ubuntu2.20
	7.35.0-1ubuntu2.20
14.04 LTS trusty	libcurl3-gnutls 7.35.0-1ubuntu2.20
	7.35.0-1ubuntu2.20
	libcurl3-nss 7.35.0-1ubuntu2.20
	7.35.0-1ubuntu2.20

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

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](#) [7.35.0-1ubuntu2.20](https://canonical.com/legal/data-privacy?cp=hide#cookies) .

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>](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>](https://canonical.com/legal/data-privacy?cp=hide#cookies) .