

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-3809-1

USN-3809-1: OpenSSH vulnerabilities

Publication date

6 November 2018

Overview

Several security issues were fixed in OpenSSH.

Releases

[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

This issue only affected Ubuntu 14.04 LTS and Ubuntu 16.04 LTS.

([CVE-2016-10708](#))

It was discovered that OpenSSH incorrectly handled certain requests.

An attacker could possibly use this issue to access sensitive information.

([CVE-2018-15473](#))

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
18.04 LTS bionic	openssh-server https://launchpad.net/ubuntu/+source/openssh – 1:7.6p1-4ubuntu0.1 https://launchpad.net/ubuntu/+source/openssh/1:7.6p1-4ubuntu0.1
16.04 LTS xenial	openssh-server https://launchpad.net/ubuntu/+source/openssh – 1:7.2p2-4ubuntu2.6 https://launchpad.net/ubuntu/+source/openssh/1:7.2p2-4ubuntu2.6
14.04 LTS trusty	openssh-server https://launchpad.net/ubuntu/+source/openssh – 1:6.6p1-2ubuntu2.11 https://launchpad.net/ubuntu/+source/openssh/1:6.6p1-2ubuntu2.11

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> .

References

- [CVE-2018-15473](#)
- [CVE-2016-10708](#)

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) .