
USN-3809-1: OpenSSH vulnerabilities

Publication date

6 November 2018

Overview

Several security issues were fixed in OpenSSH.

Releases

18.04 LTS16.04 LTS14.04 LTS

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 makVe 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>

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>