

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-4504-1

USN-4504-1: OpenSSL vulnerabilities

Publication date

16 September 2020

Overview

Several security issues were fixed in OpenSSL.

Releases

[18.04 LTS](#) [16.04 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

specification and implemented by OpenSSL contained a flaw. A remote attacker could possibly use this issue to eavesdrop on encrypted communications. This was fixed in this update by removing the insecure ciphersuites from OpenSSL. ([CVE-2020-1968](#))

Cesar Pereida García, Sohaib ul Hassan, Nicola Tuveri, Iaroslav Gridin, Alejandro Cabrera Aldaya, and Billy Brumley discovered that OpenSSL incorrectly handled ECDSA signatures. An attacker could possibly use this issue to perform a timing side-channel attack and recover private ECDSA keys. This issue only affected Ubuntu 18.04 LTS. ([CVE-2019-1547](#))

Guido Vranken discovered that OpenSSL incorrectly performed the x86_64 Montgomery squaring procedure. While unlikely, a remote...

Show more

Update instructions

After a standard system update you need to reboot your computer to 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	libssl1.0.0 < https://launchpad.net/ubuntu/+source/openssl1.0 > –
	1.0.2n-1ubuntu5.4 < https://launchpad.net/ubuntu/+source/openssl1.0/1.0.2n-1ubuntu5.4 >
	libssl1.0.0 < https://launchpad.net/ubuntu/+source/openssl > –

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>> .

[Get Ubuntu Pro](#)

References

- [CVE-2020-1968](#)
- [CVE-2019-1563](#)
- [CVE-2019-1551](#)
- [CVE-2019-1547](#)

Related notices

- [USN-7018-1](#)
- [USN-4376-1](#)
- [USN-4376-2](#)

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) .