
USN-4504-1: OpenSSL vulnerabilities

Publication date

16 September 2020

Overview

Several security issues were fixed in OpenSSL.

Releases

18.04 LTS16.04 LTS

---

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> –

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>