TLP:GREEN

Critical vulnerability in libssh CVE-2018-10933

October 18, 2018

Summary

There is a critical vulnerability in libssh, allowing a remote attacker to bypass authentication and log in without providing a password. While no major ssh server implementations use libssh, there are many appliances and IoT devices which provide remote administration using the ssh protocol. Many of these implement the remote administration feature using libssh and are consequently vulnerable.

This comm provides technical details about the vulnerability, and reliable, high fidelity methods for detecting the vulnerable services remotely.

What happened

Libssh is a library providing support for ssh and ssh2 protocols for both ssh clients and ssh servers. It allows developers to build software with support for ssh protocol, without having to deal with low level complexities of the protocol.

A critical vulnerability in libssh was disclosed on October 17, 2018 as CVE-2018-10933. This vulnerability allows a specially crafted malicious client to bypass authentication for any vulnerable libssh-based server. The vulnerability affects all versions of libssh from (inclusive) 6.0 to 0.7.5 in the 0.7 branch, and 0.8.4 in the 0.8 branch.

What is vulnerable

Vulnerability is present in any ssh **server** software built using libssh.

The ssh protocol is widely used for remote access to unix based servers, administrative interfaces for various network appliances and IoT devices. Most popular SSH server software (OpenSSH, Dropbear SSHD) *are not* vulnerable because they do not use libssh.

A review of github repositories shows only a handful of software projects using libssh to implement ssh server functionality. Most of those are small demo projects, and none are in widespread use.

However, some manufacturers of network, security, and storage appliances, as well as various IoT devices implement their remote administration with a custom ssh server, developed using libssh, making these devices vulnerable.

Available data suggests that some devices made by Fortinet appear to be vulnerable. There are unconfirmed reports of network storage appliances, firewalls, and routers that are also reportedly confirmed as vulnerable.

We were able successfully exploit a vulnerable Nutanix device. We expect other vulnerable devices to be found with thorough scanning.

On detecting the vulnerability

While ssh normally runs on port 22, the vulnerable ssh servers often run on custom ports, most commonly 2222. Ensure your scanning takes that into account.

In some cases the vulnerability can be identified by examining the server banner. By default, ssh servers using libssh will identify themselves with the string "libssh" in the server banner.

It is possible to comprehensively identify the vulnerability remotely by sending a specially crafted sequence of ssh messages. blueintel developed a small, reliable scanner you can use to quickly identify vulnerable devices both inside, and outside the perimeter. The scanner is available at https://github.com/trbpnd/bpnd-libssh.

Some enterprise vulnerability scanners published plugins for detecting this vulnerability late last night. Fidelity of these plugins is currently unknown.

Why do we care?

This is relevant because it is a high severity vulnerability, in the types of appliances likely to be 'off the radar' for security visibility.

Possible actions

1. Scan internal and external ranges for (at least) ports 22 and 2222 and identify any vulnerable devices.
2. libssh version 0.8.4 and libssh version 0.7.6 have been released to address this issue. Contact the vulnerable device manufacturer for details on patching.

References

- Original advisory: https://www.libssh.org/security/advisories/CVE-2018-10933.txt
- blueintel scanner: https://github.com/trbpnd/bpnd-libssh
- Nessus plugin: https://www.tenable.com/blog/libssh-vulnerable-to-authentication-bypass-cve-2018-10933