TLP:GREEN

Critical vulnerability in libssh CVE-2018-10933 update 1

October 19, 2018

This is an update to blueintel comm-181018.01 - “Critical vulnerability in libssh CVE-2018-10933”

Summary

Several vendors published advisories indicating their products are vulnerable to CVE-2018-10933. Major enterprise vendors whose products appear vulnerable include Cisco and F5. We also identified additional factors affecting exploitability, and we have some data points on fidelity of vulnerability scanning vendor methods of detecting this vulnerability. It is worth noting that “paramiko” - a popular python library implementing SSH protocol is vulnerable to the exact same vulnerability in the exact same way. Paramiko vulnerability was disclosed on September 6th, 2018.

This comm provides situational update on this developing Event.

Major vendors disclose vulnerability

As predicted, the vulnerability is thus far discovered in appliances. Links to vendor advisories are in the “references” section.

We have unconfirmed reports that some Blue Coat devices may be vulnerable as well, and we continue to receive unconfirmed reports of vulnerable firewalls, switches, routers, and security appliances.

On exploitability

“Vulnerable” and “exploitable” are often two different things, and that is to a large degree true with this vulnerability. Technical details are laid out in the attached TLP:GREEN document “20181019.blueintel.libssh_analysis.pdf”. To summarize:

- Some vulnerable implementations are not exploitable
- Some (and likely, most) implementations are only exploitable for a certain ssh subsystem (e.g. we can’t open a shell, but we can open SFTP session, or we can forward traffic through the vulnerable machine using ssh forwarding)

We are not aware of any vulnerable ssh server for which the vulnerability is exploitable to open a shell. We are not aware of any confirmed exploitation of any subsystem in the wild.

We are aware of several instances of successful exploitation using SFTP subsystem by blueintel and several other researchers.

On vulnerability scanners

Some vulnerability scanning vendors limit the way they check for this vulnerability by simply parsing the SSH header and looking for the string 'libssh'. As mentioned in the original comm, this is a very poor method of determining vulnerability, as it's trivial for the developer to change this header arbitrarily. One useful data point in this regard is that none of the confirmed vulnerable services we are aware of self identify as 'libssh'.

Other vulnerability scanning vendors are approaching the problem through authenticated scans, presumably enumerating binaries and looking for anything linked against libssh. While this is a far better method than the banner grabbing one, it's still prone to both false positives and false negatives.

False negatives would stem from the fact that devices likely to be vulnerable are not the types of devices you can run authenticated scans against (e.g. scanner can't log into an appliance and examine it's binaries). False positives are likely because this approach to scanning has a difficult time differentiating between 'linked against libssh' and 'linked against libssh AND using the vulnerable calls, in a vulnerable way', resulting in everything linked against libssh as being declared vulnerable, when that is certainly not the case.

bpnd-libssh remains the highest fidelity detection method we're aware of.

On public exploits

Exploits published so far are Proof-of-Concept toys, exclusively focused on attempting to open an interactive shell. There are currently no known vulnerable services against which this approach would work. Even if such services are eventually found, the currently published exploits seem unlikely to be functional.

Possible actions

- Perform a scan of internal and external ranges using bpnd-libssh. Report any findings to blueintel

References

- Cisco advisory: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181019-libssh
- F5 advisory: https://support.f5.com/csp/article/K52868493
- blueintel bpnd-libssh scanner: https://github.com/trbpnd/bpnd-libssh