July 17, 2024

Overall Rating: High

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware OpenSSH published a security advisory to address a critical vulnerability in the following product:

- OpenSSH – versions 8.5p1 to 9.7p1

Technical Details

```
A critical vulnerability in sshd(8) was present in Portable OpenSSH
versions between 8.5p1 and 9.7p1 (inclusive) that may allow arbitrary
code execution with root privileges.

Successful exploitation has been demonstrated on 32-bit Linux/glibc
systems with ASLR. Under lab conditions, the attack requires on
average 6-8 hours of continuous connections up to the maximum the
server will accept. Exploitation on 64-bit systems is believed to be
possible but has not been demonstrated at this time. It's likely that
these attacks will be improved upon.

Exploitation on non-glibc systems is conceivable but has not been
examined. Systems that lack ASLR or users of downstream Linux
distributions that have modified OpenSSH to disable per-connection
ASLR re-randomisation (yes - this is a thing, no - we don't
understand why) may potentially have an easier path to exploitation.
OpenBSD is not vulnerable.
```

This vulnerability is rated as a **HIGH** risk. A software update exists to address this risk.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have at vulnerabilityandriskmanagement@gov.bc.ca

References

- OpenSSH 9.8/9.8p1 Release Notes
- OpenSSH