Overall Rating - Critical

BRITISH COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware the PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.)

NOTE: this issue exists because of an incomplete fix for CVE-2016-10009.

Technical Details

See links below for full details.

This vulnerability is rated as a **Critical** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- Ensure mitigation is performed as soon as possible.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-38408
- https://github.com/openbsd/src/commit/7bc29a9d5cd697290aa056e94ecee6253d3425f8
- https://www.openssh.com/txt/release-9.3p2
- https://www.qualys.com/2023/07/19/cve-2023-38408/rce-openssh-forwarded-ssh-agent.txt
- https://blog.qualys.com/vulnerabilities-threat-research/2023/07/19/cve-2023-38408-remote-code-execution-in-opensshs-forwarded-ssh-agent
- https://news.ycombinator.com/item?id=36790196
- https://github.com/openbsd/src/commit/f8f5a6b003981bb824329dc987d101977beda7ca
- https://github.com/openbsd/src/commit/f03a4faa55c4ce0818324701dadbf91988d7351d
- https://www.openssh.com/security.html
- https://security.gentoo.org/glsa/202307-01
- http://www.openwall.com/lists/oss-security/2023/07/20/1
- http://www.openwall.com/lists/oss-security/2023/07/20/2
- http://packetstormsecurity.com/files/173661/OpenSSH-Forwarded-SSH-Agent-Remote-Code-Execution.html
- https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/RAXVQS6ZYTULFAK3TEJHRLKZALJS3AOU/

- https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/CEBTJJINE2I3FHAUKKNQWMFGYMLSMWKQ/
- https://security.netapp.com/advisory/ntap-20230803-0010/
- https://lists.debian.org/debian-lts-announce/2023/08/msg00021.html
- http://www.openwall.com/lists/oss-security/2023/09/22/9
- http://www.openwall.com/lists/oss-security/2023/09/22/11