10 years CERT-EU

Security Advisory 2023-051

RCE Vulnerability in “ssh-agent” of OpenSSH

July 20, 2023 — v1.0

TLP:CLEAR

History:

- *20/07/2023 — v1.0 – Initial publication*

Summary

On July 19, 2023, OpenSSH released an update regarding a vulnerability, identified as `CVE-2023-38408`. This vulnerability was discovered by the Qualys Security Advisory team and allows a remote attacker to potentially execute arbitrary commands on vulnerable OpenSSH’s forwarded `ssh-agent` [1].

`ssh-agent` is a program to hold private keys used for public key authentication. Through the use of environment variables, the agent can be located and automatically used for authentication when logging in to other machines using SSH [2].

Technical Details

The PKCS#11 support `ssh-agent` could be abused to achieve remote code execution via a forwarded agent socket if the following conditions are met:

- Exploitation requires the presence of specific libraries on the victim system.
- Remote exploitation requires that the agent was forwarded to an attacker-controlled system [3].

Affected Products

`ssh-agent` in OpenSSH between 5.5 and 9.3p1 (inclusive) [3].

Recommendations

CERT-EU recommends to install the latest updated OpenSSH 9.3p2 version [3].

Workarounds

Exploitation can also be prevented by starting `ssh-agent` with an empty PKCS#11/FIDO allow-list (`ssh-agent -P ''`) or by configuring an allow-list that contains only specific provider libraries [3].

References

[1] https://blog.qualys.com/vulnerabilities-threat-research/2023/07/19/cve-2023-38408-remote-code-execution-in-opensshs-forwarded-ssh-agent

[2] https://man.openbsd.org/ssh-agent.1

[3] https://www.openssh.com/security.html