CERT-EU

Security Advisory 2023-008

Vulnerability in OpenSSH

February 8, 2023 — v1.0

TLP:CLEAR

History:

- *08/02/2023 — v1.0 – Initial publication*

Summary

The development team of the OpenSSH suite has released the version 9.2 to address several security vulnerabilities, including a memory safety bug in the OpenSSH server (`sshd`) tracked as **CVE-2023-25136**. This vulnerability can be exploited by a remote attacker to execute arbitrary code on the target system [1].

Technical Details

The flaw was introduced in OpenSSH 9.1 and it is a pre-authentication double-free memory fault in the chunk of memory freed twice, during `options.kex_algorithms` handling. An unauthenticated attacker can trigger the double-free in the default configuration.

The vendor believes that exploitation of this vulnerability has limitations as it occurs in the unprivileged pre-auth process that is subject to chroot and is further sandboxed on most major platforms.

Affected Products

OpenSSH server (`sshd`) version 9.1 is affected.

Recommendations

CERT-EU recommends updating to OpenSSH version 9.2.

References

[1] https://nvd.nist.gov/vuln/detail/CVE-2023-25136