CERT-EU

Security Advisory 2024-039

Critical Putty Client Vulnerability

April 16, 2024 — v1.0

TLP:CLEAR

History:

- *16/04/2024 — v1.0 – Initial publication*

Summary

A critical vulnerability, identified as **CVE-2024-31497**, affects the PuTTY SSH client [1]. This vulnerability stems from a bias in ECDSA nonce generation when using the NIST P-521 elliptic curve. Attackers can exploit this bias to recover private keys after observing a relatively small number of ECDSA signatures.

Technical Details

PuTTY, when utilising the NIST P-521 elliptic curve, generates ECDSA nonces with the first 9 bits set to zero. This significant bias makes it feasible for attackers to employ state-of-the-art lattice-based techniques to recover the complete private key from these biased nonces after collecting around 60 valid ECDSA signatures.

Affected Products

- PuTTY versions before 0.81
- FileZilla versions from 3.24.1 to 3.66.5
- WinSCP versions from 5.9.5 to 6.3.2
- TortoiseGit versions from 2.4.0.2 to 2.15.0
- TortoiseSVN versions from 1.10.0 to 1.14.6

Recommendations

Users are urged to update their software to a fixed version immediately to mitigate the vulnerability. It is also recommended reviewing and replacing any NIST P-521 (`521-bit ECDSA`, `ecdsa-sha2-nistp521`) keys that may have been used with affected versions of PuTTY, as these keys should be considered compromised.

References

[1] https://www.chiark.greenend.org.uk/~sgtatham/putty/wishlist/vuln-p521-bias.html