مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

PuTTY SSH Client Vulnerable to Key Recovery Attack

Tracking #:432315766

Date:17-04-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a Critical vulnerability in PuTTY client that could be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

- **CVE-2024-31497**
- A critical vulnerability exists in PuTTY versions 0.68 through 0.80 that could allow attackers to recover NIST P-521 (ecdsa-sha2-nistp521) private keys. This vulnerability can be exploited to impersonate legitimate users and gain unauthorized access to servers.

Impact:

- Compromise of SSH private keys
- Unauthorized access to servers and services
- Potential supply chain attacks

Affected Products:

- PuTTY (0.68 - 0.80)
- FileZilla (3.24.1 - 3.66.5)
- WinSCP (5.9.5 - 6.3.2)
- TortoiseGit (2.4.0.2 - 2.15.0)
- TortoiseSVN (1.10.0 - 1.14.6)

Mitigations:

- Upgrade PuTTY to version 0.81 or later.
- Update FileZilla to version 3.67.0 or later.
- Update WinSCP to version 6.3.3 or later.
- Update TortoiseGit to version 2.15.0.1 or later.
- For TortoiseSVN users, use Plink from the latest PuTTY 0.81 release until a patch becomes available.
- Revoke compromised ECDSA NIST-P521 keys by removing them from ~/.ssh/authorized_keys and similar files on SSH servers.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by Vendor.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.chiark.greenend.org.uk/~sgtatham/putty/wishlist/vuln-p521-bias.html
- https://seclists.org/oss-sec/2024/q2/122