National Cyber Security Centre

2404180124-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Vulnerability in PuTTY SSH Client (CVE-2024-31497)

Thursday 18th April, 2024

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP-CLEAR information may be shared without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

Published: 2024-04-15T20:15:00
CVE ID: CVE-2024-31497
EPSS[1]**:** 0.156770000
(For up to date EPSS score, click here: https://api.first.org/data/v1/epss?cve=CVE-2024-31497)
Summary: In PuTTY 0.68 to 0.80, biased ECDSA nonce generation allows an attacker to recover a user's NIST P-521 secret key via a quick attack in approximately 60 signatures. This is especially important in a scenario where an adversary is able to read messages signed by PuTTY or Pageant. The required set of signed messages may be publicly readable because they are stored in a public Git service that supports use of SSH for commit signing, and the signatures were made by Pageant through an agent-forwarding mechanism.

In other words, an adversary may already have enough signature information to compromise a victim's private key, even if there is no further use of vulnerable PuTTY versions.

If the other services include Git services, then it may be possible to conduct supply-chain attacks on software maintained in Git.

Products Affected

- 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

Impact

After a key compromise, an adversary may be able to conduct supply-chain attacks on software maintained in Git.

A second, independent scenario is that the adversary is an operator of an SSH server to which the victim authenticates (for remote login or file copy), even though this server is not fully trusted by the victim, and the victim uses the same private key for SSH connections to other services operated by other entities.

Here, the rogue server operator (who would otherwise have no way to determine the victim's private key) can derive the victim's private key, and then use it for unauthorised access to those other services.

Present in CISA Known Exploited Vulnerability(KEV)[2] **catalog:** No

[1] https://www.first.org/epss/articles/prob_percentile_bins
[2] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommendations

The NCSC strongly advises affected organisations to review the latest release notes and update their software to a fixed version immediately to mitigate this vulnerability.

This vulnerability has been fixed in PuTTY 0.81, FileZilla 3.67.0, WinSCP 6.3.3, and TortoiseGit 2.15.0.1. Users of TortoiseSVN are advised to configure TortoiseSVN to use Plink from the latest PuTTY 0.81 release when accessing a SVN repository via SSH until a patch becomes available.

Additional recommendations and mitigation's for CVE-2024-31497 can be found in the respective links below:

- PuTTY vulnerability vuln-p521-bias
- Filezilla Versions
- Openwall Security Advisory
- CERT-EU Advisory
- WinSCP News
- TortoiseGIT

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie