

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## **Vulnerability in PuTTY Client Allows Recovery of Private Key**

Date of Publication

April 17, 2024

Admiralty Code

A1

TA Number

TA2024150


# Summary

**Discovered:** April 2024

**Affected Products:** PuTTY

**Impact:** The flaw identified as CVE-2024-31497 in PuTTY could potentially allow attackers to access the private key used to generate cryptographic signatures. This vulnerability enables remote attackers to retrieve NIST P-521 private keys.

## CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-31497	PuTTY Information Disclosure Vulnerability	PuTTY			

## Vulnerability Details

### #1

The security flaw CVE-2024-31497 poses a significant risk to PuTTY versions 0.68 through 0.80, potentially allowing attackers to access private keys used to generate cryptographic signatures. PuTTY, a widely used open-source terminal emulator and network file transfer application, is popular among system administrators and developers for remote server management tasks.

### #2

This vulnerability in PuTTY enables remote attackers to recover NIST P-521 private keys by exploiting biased ECDSA nonces generated by the PuTTY client and its components. Specifically, the flaw lies in the generation of heavily biased ECDSA nonces for NIST P-521, where the first 9 bits are consistently zero. This bias facilitates the full recovery of the secret key using advanced techniques, requiring only around 60 signatures.

## #3

Attackers can obtain these signatures from various sources, including a malicious server or signed git commits. Although some degree of bias exists in nonce generation for other curves, it is negligible and insufficient to enable similar attacks.

## #4

PuTTY version 0.81 addresses this vulnerability by implementing the RFC 6979 technique for DSA and ECDSA keys. However, private keys generated using previous vulnerable versions should be considered insecure and replaced with new, secure keys. Additionally, other software bundles such as FileZilla, WinSCP, TortoiseGit, and TortoiseSVN may also be susceptible to this vulnerability and require appropriate updates or remediation measures.

## Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-31497	PuTTY Versions 0.68 - 0.80	cpe:2.3:a:putty:putty:*:*:*:*:*	CWE-200

## Recommendations



**Update:** It's crucial to update and upgrade to PuTTY version 0.81 immediately to mitigate the vulnerability. These updates include patches to address the security flaw and enhance the overall security.



**Change the old keys:** It's crucial to retire any ECDSA private keys generated with the vulnerable version of PuTTY and replace them with new, secure keys to mitigate the risk posed by the vulnerability. Additionally, removing the old public key from all OpenSSH authorized\_keys files is an important step to ensure that only the new, secure keys are in use.



**Deploy Behavioral Analysis Solutions:** Utilize behavioral analysis solutions to detect any anomalous behavior on systems. Ensure that endpoint protection solutions are regularly updated to identify and mitigate the latest threats.



**Vulnerability Management:** Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

# Potential MITRE ATT&CK TTPs

<b><u>TA0042</u></b> Resource Development	<b><u>TA0043</u></b> Reconnaissance	<b><u>TA0006</u></b> Credential Access	<b><u>T1588</u></b> Obtain Capabilities
<b><u>T1588.006</u></b> Vulnerabilities	<b><u>T1592</u></b> Gather Victim Host Information	<b><u>T1552</u></b> Unsecured Credentials	<b><u>T1552.004</u></b> Private Keys
<b><u>T1212</u></b> Exploitation for Credential Access			

## Patch Details

Update to the latest version of PuTTY, version 0.81 to address the flaw CVE-2024-31497.

Link: <https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>

## References

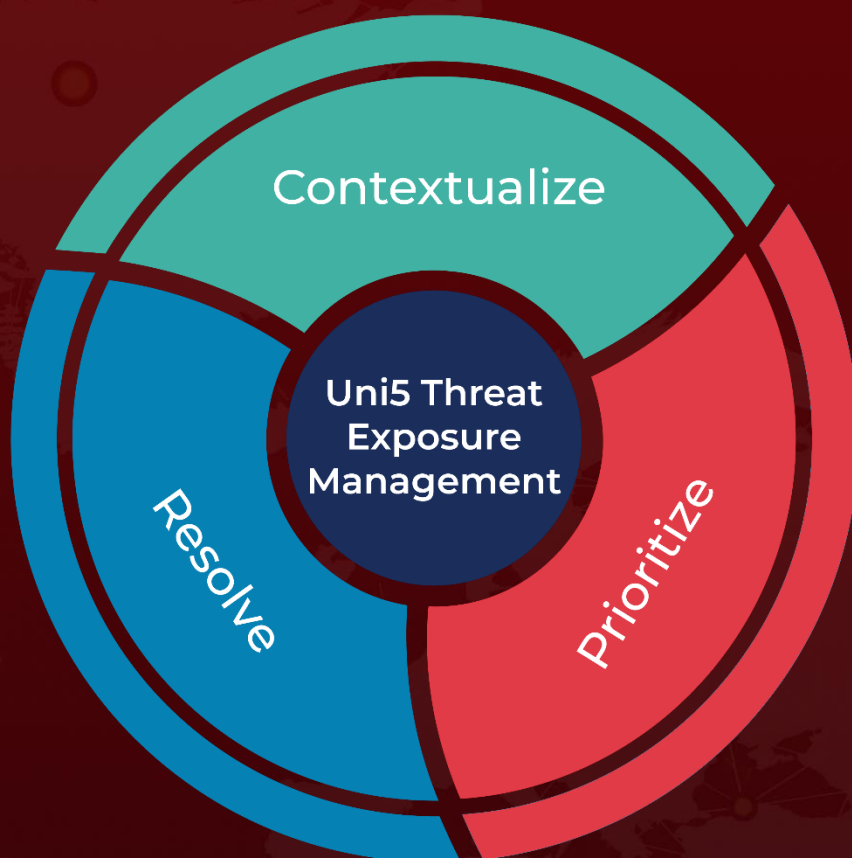
<https://www.chiark.greenend.org.uk/~sgtatham/putty/wishlist/vuln-p521-bias.html>

<https://www.openwall.com/lists/oss-security/2024/04/15/6>

# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

**April 17, 2024 • 5:45 AM**

© 2024 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)