Cal OES
GOVERNOR'S OFFICE OF EMERGENCY SERVICES

CYBER ADVISORY

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

*CYBER ADVISORY*

TLP:CLEAR
16 April 2024

## PuTTY Biased ECDSA Vulnerability

CVE-2024-31497 PuTTY NIST P-521 Critical Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware a critical vulnerability under active exploitation known as CVE-2024-31497.[1] The vulnerability lies in PuTTY versions PuTTY 0.68 through 0.80.[2,3] Exploitation of the vulnerability may generate heavily biased Elliptic Curve Digital Signature Algorithm (ECDSA) nonces[4] in the case of NIST P-521, which enables full secret key recovery. All NIST P-521 client keys used with PuTTY must be considered compromised, given that the attack can be carried out even after the root cause has been fixed in the source code.[5]

The Cal-CSIC recommends immediately patching to PuTTY version 0.81.

For further information on applying PuTTY recommended patches please refer to PuTTY.git.

### Organization, Source, Reference, and Dissemination Information

| | |
|---|---|
| **Organization Description** | California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state. |
| **Customer Feedback** | If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback calcsic@caloes.ca.gov. |

**WARNING:** This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

| | |
|---|---|
| **Source Summary Statement** | This report was compiled from a variety of sources, predominately open-source reporting. |
| **Handling Caveats** | **Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction. |
| **Information Needs** | *HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5* |

[1] Security Week; "Critical PuTTY Vulnerability Allows Secret Key Recovery;" https://www.securityweek.com/critical-putty-vulnerability-allows-secret-key-recovery/; accessed 16 April 2024

[2] NIST; "Elliptic Curve Digital Signature Algorithm;" https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Standards-and-Guidelines/documents/examples/P521_SHA512.pdf; accessed 16 April 2024

[3] Green End; "PuTTY vulnerability vuln-p521-bias;" https://www.chiark.greenend.org.uk/~sgtatham/putty/wishlist/vuln-p521-bias.html; accessed 16 April 2024

[4] Nonce: In cryptography, a nonce is a random number that can be used only once in a cryptographic communication

[5] Red Hat; "Bug 2275183 (CVE-2024-31497) - CVE-2024-31497 putty: secret key recovery of NIST P-521 private keys through biased ECDSA nonces in putty client;" https://bugzilla.redhat.com/show_bug.cgi?id=2275183; accessed 16 April 2024