GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

14 September 2026

Advisory 310: SSH "Terrapin" Prefix-Truncation Protocol Weakness — Still Being Detected on Internet-Exposed Servers (CVE-2023-48795).

Release Date: 18th December 2023
Impact: MEDIUM
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that operate any SSH server or client, including OpenSSH, PuTTY, and libssh-based products. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2023-48795, known as the "Terrapin attack," is a protocol-level weakness in the SSH transport protocol itself, publicly disclosed on 18 December 2023 and affecting essentially every SSH implementation in widespread use, including OpenSSH, PuTTY, libssh, and others. When configured to use either the ChaCha20-Poly1305 cipher or a CBC-mode cipher combined with Encrypt-then-MAC.

CERTVU is issuing this advisory now, nearly three years after original disclosure, because CVE-2023-48795 continues to appear in the Shadowserver Foundation's "Accessible SSH" internet-scanning report - a recurring feed CERTVU monitors that identifies internet-reachable SSH servers still configured with vulnerable cipher modes.

What are the systems affected?

The following version(s) are affected:

- Any SSH server or client (including OpenSSH prior to 9.6, PuTTY, libssh, and other implementations) configured to allow the "chacha20-poly1305@openssh.com" cipher, or a CBC-mode cipher combined with "-etm@openssh.com" MAC negotiation - (Affected)

OpenSSH 9.6 and later, and other implementations supporting the "strict key exchange" countermeasure (published December 2023) - (Not affected, patched, when strict key exchange is negotiated by both endpoints)

What does this mean?

Typical attack flow:

1. **Establish a man-in-the-middle position on the network path**
    - An attacker with an active man-in-the-middle position between an SSH client and server manipulates packet sequence numbers during the connection handshake, before encryption keys are fully established.
2. **Silently truncate messages at the start of the secure channel**
    - By injecting unauthenticated "ignore" messages and adjusting sequence numbers, the attacker removes an attacker-chosen number of consecutive messages from the very beginning of the secure channel without causing a MAC failure - potentially stripping security-relevant extension negotiation that neither endpoint will detect as missing.

Attack vectors:

- A network-based attack requiring the attacker to already hold an active man-in-the-middle position (CVSS AC:H) - this is not a fully remote, no-prerequisite attack, unlike most advisories CERTVU issues.
- No user interaction or privileges are required once a man-in-the-middle position is established

Successful exploitation may allow attackers to:

- Silently remove messages from the start of an SSH secure channel, without either endpoint detecting the tampering.
- Downgrade or strip security-relevant protocol extensions and certain authentication mechanisms negotiated at connection start, weakening the effective security of an otherwise-encrypted SSH session.

Mitigation process

CERTVU recommends the following:

1. Upgrade to SSH software supporting strict key exchange

    - Upgrade to OpenSSH 9.6 or later (or the equivalent fixed version of your specific SSH client/server software), noting that the fix is only effective when both endpoints of a connection support strict key exchange.

2. Disable vulnerable cipher modes where an immediate upgrade is not possible
3. Check your own exposure against Shadowserver's Accessible SSH report
4. Review SSH server configuration as part of routine hardening, not only at initial setup

Report any suspected compromise involving SSH access to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://www.cve.org/CVERecord?id=CVE-2023-48795
2. https://terrapin-attack.com/