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

19 August 2026

Advisory 193: CVE-2026-65400_Apple macOS Improper Authentication Vulnerability

Release Date: 6th August 2026
Impact: CRITICAL
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 utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-65400 is a critical-severity authentication bypass vulnerability in the Screen Sharing service (screensharingd) built into macOS, Apple's remote desktop feature reachable over TCP port 5900.
An attacker on the network can authenticate to Screen Sharing without valid credentials. The root cause lies in the service's implementation of Secure Remote Password (SRP) authentication: a frame-length validation error causes the daemon to return a stale success status, so an unauthenticated connection is treated as legitimate and continues without the expected cryptographic protection.

What are the systems affected?

Affected systems are any Mac running a pre-patch version of the three currently supported macOS releases, provided Screen Sharing is enabled.

macOS Sequoia, prior to 15.7.9 - (Affected)

macOS Sonoma, prior to 14.8.9 - (Affected)
macOS Tahoe, prior to 26.6.1 - (Affected)
Macs with Screen Sharing disabled - (Not exposed to this vector)

Any Mac with Screen Sharing enabled and port 5900 reachable from an untrusted network or the internet faces critical, confirmed risk, including Macs used for development, IT administration, or infrastructure management.

What does this mean?

This flaw requires no initial access step: the only prerequisite is that Screen Sharing is enabled on the target Mac and reachable over the network on TCP port 5900.

Step 1 - Network Reachability
The attacker reaches the target Mac's Screen Sharing service on TCP port 5900, whether over a shared local network or, in confirmed cases, directly over the internet.

Step 2 - Authentication State Desync
The attacker initiates a Secure Remote Password handshake and sends an oversized frame during validation. A length check in screensharingd's frame validator bails out early and returns the success code from a preceding read rather than a failure, advancing the state machine as though authentication succeeded.

Step 3 - Unauthenticated Privileged Access
Because the bypass occurs before authentication completes, no valid macOS account, approved Screen Sharing user, or legacy VNC password is required. The resulting session also lacks the expected cryptographic protection and runs in cleartext.

Step 4 - Root Access and Cryptomining
The attacker abuses Screen Sharing's privileged file-transfer components to read and write files as **root**. In confirmed NCSC-NL cases this was used to install a Monero cryptocurrency miner; the same file read/write primitive has also been demonstrated as a path to full remote code execution.

Mitigation process

CERTVU recommends the following:

1. **Update macOS Immediately**

Update every affected Mac to macOS Tahoe 26.6.1, macOS Sequoia 15.7.9, or macOS Sonoma 14.8.9. Because the bypass occurs in the authentication path itself, rotating Screen Sharing passwords, changing the list of approved users, or disabling legacy VNC authentication does not remediate the vulnerability - only the security update does.

Huntress Technical Analysis: macOS Screen Sharing RCE

2. **Reduce Exposure and Check for Compromise**

Where Screen Sharing is not actively required, disable it entirely via System Settings > General > Sharing rather than relying on network controls alone, and never expose it directly to the internet via port forwarding on TCP port 5900 - use a VPN for remote access instead.

Reference

1. https://thehackernews.com/2026/08/apple-macos-screen-sharing-flaw.html
2. https://www.cve.org/CVERecord?id=CVE-2026-65400
3. https://www.securityweek.com/recent-macos-screen-sharing-vulnerability-exploited-in-attacks/