Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

macOS Screen Sharing Authentication Bypass Flaw Exploited

Date of Publication	Admiralty Code	TA Number
August 18, 2026	A1	TA2026236

Summary

First Seen: August 2026
Malware: Monero Miner
Affected Products: Apple macOS Sonoma, macOS Sequoia, macOS Tahoe
Impact: Apple has patched CVE-2026-65400, a critical authentication flaw in the macOS Screen Sharing component. The flaw affects macOS Sonoma, Sequoia, and Tahoe. Shortly after the patch, active abuse was reported in the wild, with attackers targeting Macs that had the Screen Sharing port (TCP 5900) reachable from the internet, obtaining root access, and installing a Monero cryptocurrency miner. Public proof-of-concept code is also available, and reporting notes that AI-assisted tooling has sharply shortened the time between disclosure and a working exploit. Together, these factors raise the urgency for organisations to apply the update without delay.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-65400	Apple macOS Improper Authentication in Screen Sharing Vulnerability	Apple macOS (Sonoma, Sequoia, Tahoe)	✗	✗	✓

Vulnerability Details

#1

A recently patched security flaw in Apple macOS has come under active exploitation to deploy a cryptocurrency miner. Tracked as CVE-2026-65400, it is an improper authentication weakness (CWE-287) in the Screen Sharing component of macOS, Apple's built-in remote desktop service, which listens on TCP port 5900 and is based on the VNC protocol. The root cause is insufficient state management within the Screen Sharing authentication path: during the login exchange, the service's internal state can advance as though authentication had succeeded when it had not. As a result, an attacker on the network can reach an authenticated session without presenting valid credentials. Public technical reporting characterises the flaw as a state-machine desynchronisation, and notes that the only requirement is naming a valid account, which is not a secret and is often visible on the macOS login window.

#2

The attack is carried out over the network with low complexity and requires no user interaction. It is worth noting that CVE-2026-65400 is distinct from a separate pre-authentication issue in the Screen Sharing daemon that Apple addressed in the earlier macOS 26.6 release; the two flaws reside in the same source code area but are tracked separately. The vulnerability affects macOS Sonoma before 14.8.9, macOS Sequoia before 15.7.9, and macOS Tahoe before 26.6.1, and Apple resolved it by improving the state management logic so that only valid credentials are accepted, and unauthorised authentication attempts are rejected.

#3

Active exploitation has been confirmed. Received a report of abuse across multiple systems where port 5900 was internet-facing; in each case attackers gained root and installed a Monero crypto miner. Public reporting cautions that details on the timing, scale, and precise mechanism of these attacks remain limited, and that it is not established whether the flaw was exploited before the patch was available. Given the confirmed exploitation activity, organisations running affected macOS versions should update to the latest release without delay to stay protected.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-65400	Apple macOS Sonoma (Before 14.8.9), macOS Sequoia (Before 15.7.9), macOS Tahoe (Before 26.6.1)	cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*	CWE-287

Recommendations

Update macOS Immediately: Install Apple's emergency updates without delay, macOS Tahoe 26.6.1, macOS Sequoia 15.7.9, or macOS Sonoma 14.8.9, depending on the version in use. These releases fix the authentication flaw and are the most effective way to close the exposure.

Disable or Restrict Screen Sharing: If patching cannot be done right away, turn off Screen Sharing by navigating to General > Sharing and toggling Screen Sharing off. Never expose TCP port 5900 directly to the internet; if remote access is required, place the service behind a VPN or SSH tunnel and limit it to trusted source addresses.

Hunt for Signs of Compromise: On systems that were internet-facing, look for indicators of the observed activity, such as unfamiliar processes consuming high CPU, unexpected cryptominer binaries, unexplained root-level activity, and unauthorised changes to sudoers or other privileged configuration. Systems confirmed as compromised should be isolated, investigated, and rebuilt rather than only cleaned.

Reduce Network Exposure: Audit the environment for any Macs reachable from the internet on port 5900 and remove that exposure. Apply network segmentation and firewall rules so that remote desktop services are only reachable from managed, trusted networks.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1133: External Remote Services	
	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	
Impact	T1496: Resource Hijacking	T1496.001: Compute Hijacking
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Patch Links

https://support.apple.com/en-us/148170

https://support.apple.com/en-us/148171

https://support.apple.com/en-us/148172

References

https://advisories.ncsc.nl/2026/ncsc-2026-0280.html

https://support.apple.com/en-us/148170

https://support.apple.com/en-us/148171

https://support.apple.com/en-us/148172

https://blog.calif.io/p/no-country-for-old-passwords

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 Demo of **HivePro**.

REPORT GENERATED ON

August 18, 2026 • 08:00 AM

More at www.hivepro.com