Actively Exploited Apple macOS Screen Sharing Vulnerability Allows Root Access

Author: *Portia S. Cole – CTI Researcher*

TL;DR

There is a critical vulnerability (CVE-2026-65400, CVSS 9.8) in Apple macOS Screen Sharing that allows a remote attacker to access an affected Mac without valid credentials.

Public exploit code is available, and attackers are exploiting the vulnerability on systems with Screen Sharing exposed to the internet. Reported attacks obtained root access and installed Monero cryptominers.

Overview

There is a vulnerability (CVE-2026-65400, CVSS 9.8) in Apple macOS Screen Sharing that allows an attacker with network access to bypass authentication and connect without a valid username or password. The vulnerability can be exploited remotely without privileges or user interaction.

Screen Sharing is a built-in macOS service that allows authorized users to view and remotely control a Mac. The service commonly uses TCP port 5900. The vulnerability can be exploited when Screen Sharing is enabled and reachable over the network. Internet-facing Macs are easier to target, while internal Macs could be attacked by someone who has already accessed the organization's network.

Affected Products

Apple addressed the vulnerability in the following releases:

- macOS Tahoe 26.6.1
- macOS Sequoia 15.7.9
- macOS Sonoma 14.8.9

Apple fixed the vulnerability in updates for macOS Tahoe, Sequoia and Sonoma. However, public exploit code is available, and the Netherlands NCSC confirmed attacks against internet-facing Macs in which attackers gained root access and installed Monero cryptominers. The attacker and number of compromised systems remain unknown.

Impact on Aspire Customers

This issue is most relevant to customers that use Screen Sharing for remote access or IT support. Macs with port 5900 exposed to the internet are the easiest targets, though internal systems could also be attacked after a network compromise.

Root access could allow an attacker to steal data or credentials and install more malware. The Monero miner seen in these attacks may also slow affected Macs and disrupt normal work.

Aspire Protects

- **Patch** – Update affected Macs to macOS Tahoe 26.6.1, macOS Sequoia 15.7.9, macOS Sonoma 14.8.9 or later.
- Disable Screen Sharing on systems where it is not required.
- Block internet access to TCP port 5900. If Screen Sharing is required, restrict access through a secured VPN or approved source addresses.
- Identify and investigate unpatched Macs that had TCP port 5900 exposed to the internet. Isolate systems showing unauthorized root access or cryptomining activity.

TTPs to Watch

Initial Access

- External Remote Services [T1133]: An attacker may exploit an internet-accessible Screen Sharing service to access a vulnerable Mac without valid credentials.

Impact

- Compute Hijacking [T1496.001]: An attacker may install a cryptocurrency miner that uses the compromised Mac's processing resources to mine Monero.

IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

The vulnerability can affect any organization operating a vulnerable Mac with Screen Sharing enabled, including:

- Public Sector
- Energy
- Legal & Professional Services
- Healthcare
- Finance
- Education

- Retail
- Manufacturing

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.

- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company's reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

About the security content of macOS Sonoma 14.8.9 - Apple Support

About the security content of macOS Sequoia 15.7.9 - Apple Support

About the security content of macOS Tahoe 26.6.1 - Apple Support