



NCSC-2026-0280

Kwetsbaarheid verholpen in macOS Screen Sharing door Apple

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 12-08-2026

Revisie: 1.0.1

TLP:WHITE

Toegestane verspreiding van TLP:WHITE

(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Update Revisie 1

Publieke PoC code beschikbaar en actief misbruik bekend

Feiten

Apple heeft een kwetsbaarheid verholpen in de Screen Sharing feature van macOS versies Sequoia 15.7.9, Sonoma 14.8.9 en Tahoe 26.6.1.

Duiding

De kwetsbaarheid betreft een authenticatieprobleem in de Screen Sharing functionaliteit waarbij netwerkaanvallers toegang kunnen verkrijgen zonder geldige inloggegevens. Dit wordt mogelijk gemaakt door onvoldoende state management tijdens het authenticatieproces. Hierdoor kunnen onbevoegden authenticatiepogingen uitvoeren die normaal niet geaccepteerd zouden worden.

Update: Het NCSC heeft een melding ontvangen waaruit blijkt dat er actief misbruik van deze kwetsbaarheid is waargenomen op meerdere systemen waarop poort 5900 vanaf het internet bereikbaar was. In al deze gevallen was root toegang verkregen op het getroffen systeem en een Monero crypto miner geplaatst.

Oplossingen

Apple heeft de state management mechanismen verbeterd om correcte validatie van inloggegevens af te dwingen en ongeautoriseerde authenticatiepogingen te voorkomen. Updates zijn uitgebracht die ervoor zorgen dat alleen geldige inloggegevens worden geaccepteerd. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://support.apple.com/en-us/148170>
- <https://support.apple.com/en-us/148171>
- <https://support.apple.com/en-us/148172>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-65400	7.1 HIGH

CWE's

CWE	Beschrijving
CWE-287	Improper Authentication

Getroffen producten

Apple
macOS Sequoia
macOS Sonoma
macOS Tahoe

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.