Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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 kwetbaarheid 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