



Advisory NCSC-2025-0032

Kwetsbaarheden verholpen in Apple macOS

2025-01-28 Revisie 0

Toegestande verspreiding: 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 mogen de informatie delen met collega's van andere organisaties, informatiefora of personen werkzaam in netwerkbeveiliging, informatiebeveiliging of de VI-gemeenschap in de bredere zin. Het is niet de bedoeling dat u de informatie publiek maakt.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Apple heeft kwetsbaarheden verholpen in macOS Ventura (Specifiek voor versies 13.7.3), Sequoia (Specifiek voor versies 15.3) en Sonoma (Specifiek voor versies 14.7.3).

Interpretaties

De kwetsbaarheden omvatten verschillende problemen, waaronder ongeautoriseerde toegang tot gevoelige gebruikersdata, onjuiste permissies, en kwetsbaarheden die kunnen leiden tot onverwachte applicatie-terminaties. De updates bevatten verbeterde validatietechnieken en extra beveiligingsmaatregelen om de integriteit van gebruikersdata te waarborgen en de algehele beveiliging van de systemen te versterken.

Oplossingen

Apple heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://support.apple.com/en-us/122074>
- <https://support.apple.com/en-us/122070>
- <https://support.apple.com/en-us/122069>
- <https://support.apple.com/en-us/122068>