



## Advisory NCSC-2025-0034

# Kwetsbaarheden verholpen in Apple iPadOS en iOS

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](http://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](mailto:info@ncsc.nl)

## Feiten

Apple heeft kwetsbaarheden verholpen in iOS en iPadOS.

---

## Interpretaties

De kwetsbaarheden omvatten onder andere problemen met geheugenbeheer, invoervalidatie, en de verwerking van webinhoud, die konden leiden tot ongeautoriseerde toegang, executie van willekeurige code en Denial-of-Service aanvallen. Apple geeft aan dat CVE-2025-24085, die kan worden misbruikt om verhoogde rechten te verkrijgen op het systeem, mogelijkertwijze actief is misbruikt.

---

## Oplossingen

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

---

## Referenties

- <https://support.apple.com/en-us/122066>
- <https://support.apple.com/en-us/122067>