



## Advisory NCSC-2024-0382

# Kwetsbaarheden verholpen in Apple iOS en iPadOS

2024-09-26 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

Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot de volgende categorieën schade:

- Cross-Site-Scripting (XSS)
- Denial-of-Service (DoS)
- Manipulatie van gegevens
- Omzeilen van beveiligingsmaatregel
- Toegang tot gevoelige gegevens
- Toegang tot systeemgegevens

Voor succesvol misbruik moet de kwaadwillende fysieke toegang hebben tot het kwetsbare apparaat, het slachtoffer misleiden een malafide app te installeren en draaien of een malafide link te volgen.

---

## Oplossingen

Apple heeft updates uitgebracht om de kwetsbaarheden te verhelpen in iOS en iPadOS 17.7 en 18. Zie bijgevoegde referenties voor meer informatie.

---

## Referenties

- <https://support.apple.com/en-us/121250>
- <https://support.apple.com/en-us/121246>