Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2024-0457

Kwetsbaarheden verholpen in Apple iOS en iPadOS

2024-11-20 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.firs t.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 meerdere kwetsbaarheden verholpen in iOS en iPadOS.

Interpretaties

Twee kwetsbaarheden in iOS en iPadOS 17.7.2 (CVE-2024-44308 & CVE-2024-44309) kunnen leiden tot het uitvoeren van willekeurige code. Apple geeft aan dat actief misbruik van deze kwetsbaarheden bekend is.

Een kwaadwillende kan de kwetsbaarheden in iOS en iPadOS 18 misbruiken om aanvallen uit te voeren die kunnen leiden tot de volgende categorieën schade:

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

Oplossingen

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

Referenties

- https://support.apple.com/en-us/121754
- https://support.apple.com/en-us/121250