Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2024-0319

Kwetsbaarheden verholpen in Apple iOS en iPadOS

2024-07-30 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 kwetsbaarheden verholpen in iOS en iPadOS.

Interpretaties

Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot een Denial-of-Service, toegang tot systeemgegevens of toegang tot gevoelige gegevens.

Om toegang te krijgen tot gevoelige gegevens, moet de kwaadwillende fysieke toegang hebben tot het kwetsbare systeem. Om een Denial-of-Service te veroorzaken, of systeemgegevens te bemachtigen moet de kwaadwillende het slachtoffer misleiden een malafide app te installeren en draaien.

Oplossingen

Apple heeft updates uitgebracht om de kwetsbaarheden te verhelpen in iOS en iPadOS 16.7.9 & 17.6. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://support.apple.com/en-us/HT214116
- https://support.apple.com/en-us/HT214117