Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0487

Kwetsbaarheden verholpen in Apple iPadOS en iOS

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 12-12-2024

TLP:WHITE

Toegestane verspreiding van 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 van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Apple heeft kwetsbaarheden verholpen in iPadOS (Specifiek voor versies 17.7.3 en 18.2) en iOS (Specifiek voor 18.2).

Duiding

De kwetsbaarheden omvatten onder andere een denial-of-service probleem, logica-issues die ongeautoriseerde privilege-escalatie mogelijk maakten, en onverwachte systeemterminaties door geheugen-corruptie. Deze kwetsbaarheden konden worden misbruikt door kwaadwillenden via het verwerken van kwaadwillig vervaardigde bestanden, webinhoud of afbeeldingen. De updates verbeteren de algehele stabiliteit en beveiliging van de systemen door verbeterde geheugenbeheertechnieken en validatiecontroles te implementeren.

Oplossingen

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

Referenties

- https://support.apple.com/en-us/121838
- https://support.apple.com/en-us/121837

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-44201	
CVE-2024-44225	
CVE-2024-44245	
CVE-2024-44246	
CVE-2024-45490	9.8 CRITICAL
CVE-2024-54479	

- CVE-2024-54485
- CVE-2024-54486
- CVE-2024-54492
- CVE-2024-54494
- CVE-2024-54500
- CVE-2024-54501
- CVE-2024-54502
- CVE-2024-54503
- CVE-2024-54505
- CVE-2024-54508
- CVE-2024-54510
- CVE-2024-54513
- CVE-2024-54514
- CVE-2024-54526
- CVE-2024-54527
- CVE-2024-54534

CWE's

CWE	Beschrijving
CWE-131	Incorrect Calculation of Buffer Size
CWE-265	CWE-265
CWE-190	Integer Overflow or Wraparound
CWE-275	CWE-275
CWE-284	Improper Access Control

CWE-611	Improper Restriction of XML External Entity Reference

Getroffen producten

apple
ios_and_ipados
ipados
ios

Disclaimer