Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0382

Kwetsbaarheden verholpen in Apple iOS en iPadOS

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 26-09-2024

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 iOS en iPadOS.

Duiding

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

Kwetsbaarheden

CVE	CVSS Score
CVE-2023-5841	9.1 CRITICAL
CVE-2024-27869	7.5 HIGH
CVE-2024-27874	7.5 HIGH
CVE-2024-27876	8.1 HIGH

CVE-2024-27879	7.5 HIGH
CVE-2024-27880	5.5 MEDIUM
CVE-2024-40791	3.3 LOW
CVE-2024-40826	6.1 MEDIUM
CVE-2024-40830	3.3 LOW
CVE-2024-40840	4.6 MEDIUM
CVE-2024-40844	5.5 MEDIUM
CVE-2024-40850	5.5 MEDIUM
CVE-2024-40852	7.5 HIGH
CVE-2024-40856	7.5 HIGH
CVE-2024-40857	7.1 HIGH
CVE-2024-40863	5.5 MEDIUM
CVE-2024-44124	6.5 MEDIUM
CVE-2024-44127	5.3 MEDIUM
CVE-2024-44131	5.5 MEDIUM
CVE-2024-44139	
CVE-2024-44147	7.7 HIGH
CVE-2024-44158	5.5 MEDIUM
CVE-2024-44164	
CVE-2024-44165	
CVE-2024-44167	8.1 HIGH
CVE-2024-44169	8.1 HIGH
CVE-2024-44170	

CVE-2024-44171	**4.6 MEDIUM**
CVE-2024-44176	**5.5 MEDIUM**
CVE-2024-44180	
CVE-2024-44183	
CVE-2024-44184	**5.5 MEDIUM**
CVE-2024-44187	**6.5 MEDIUM**
CVE-2024-44191	**5.5 MEDIUM**
CVE-2024-44198	**5.5 MEDIUM**
CVE-2024-44202	

CWE's

CWE	Beschrijving
CWE-942	Permissive Cross-domain Policy with Untrusted Domains
CWE-190	Integer Overflow or Wraparound
CWE-285	Improper Authorization
CWE-404	Improper Resource Shutdown or Release
CWE-275	CWE-275
CWE-284	Improper Access Control
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-122	Heap-based Buffer Overflow
CWE-287	Improper Authentication
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

apple
ios__17.7
ios__18
ipados__17.7
ipados__18

Disclaimer