



NCSC-2024-0457

Kwetsbaarheden verholpen in Apple iOS en iPadOS

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 20-11-2024

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 meerdere kwetsbaarheden verholpen in iOS en iPadOS.

Duiding

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>

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-2024-40850	5.5 MEDIUM
> CVE-2024-40852	7.5 HIGH
> CVE-2024-40853	
> CVE-2024-40856	7.5 HIGH
> CVE-2024-40857	7.1 HIGH
> CVE-2024-40863	5.5 MEDIUM
> CVE-2024-44123	
> CVE-2024-44124	6.5 MEDIUM
> CVE-2024-44126	
> CVE-2024-44127	5.3 MEDIUM
> CVE-2024-44131	5.5 MEDIUM
> CVE-2024-44139	
> CVE-2024-44144	
> CVE-2024-44145	
> CVE-2024-44147	7.7 HIGH
> CVE-2024-44155	
> CVE-2024-44165	7.5 HIGH

> CVE-2024-44167	8.1 HIGH
> CVE-2024-44169	8.1 HIGH
> CVE-2024-44170	5.5 MEDIUM
> 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	
> CVE-2024-44217	

CWE's

CWE	Beschrijving
> CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
> 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-787	Out-of-bounds Write
› CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
› CWE-122	Heap-based Buffer Overflow
› CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
› CWE-287	Improper Authentication

Getroffen producten

apple
ipados__17.7
ipados__18
ios__18
ios__17.7

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.