



# 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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto: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
➤ <a href="#">CVE-2023-5841</a>	9.1 CRITICAL
➤ <a href="#">CVE-2024-27869</a>	7.5 HIGH
➤ <a href="#">CVE-2024-27874</a>	7.5 HIGH
➤ <a href="#">CVE-2024-27876</a>	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
> CVE-942	Permissive Cross-domain Policy with Untrusted Domains
> CVE-190	Integer Overflow or Wraparound
> CVE-285	Improper Authorization
> CVE-404	Improper Resource Shutdown or Release
> CVE-275	CWE-275
> CVE-284	Improper Access Control
> CVE-200	Exposure of Sensitive Information to an Unauthorized Actor
> CVE-122	Heap-based Buffer Overflow
> CVE-287	Improper Authentication
> CVE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

## Getroffen producten

<b>apple</b>
ios__17.7
ios__18
ipados__17.7
ipados__18

## 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.