



NCSC-2025-0103

Kwetsbaarheden verholpen in Apple iOS en iPadOS

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 01-04-2025

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

De kwetsbaarheden omvatten onder andere geheugenbeheerproblemen, ongeautoriseerde toegang tot gevoelige gebruikersdata, en de mogelijkheid voor applicaties om hun sandbox-omgevingen te ontsnappen. Deze kwetsbaarheden konden leiden tot ongeautoriseerde toegang, gegevenswijzigingen, of zelfs Denial-of-Service. Voor succesvol misbruik moet de kwaadwillende het slachtoffer misleiden een malafide app te installeren of link te volgen.

Oplossingen

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

Referenties

- <https://support.apple.com/en-us/122345>
- <https://support.apple.com/en-us/122346>
- <https://support.apple.com/en-us/122372>
- <https://support.apple.com/en-us/122371>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-24217	
➤ CVE-2025-24221	
➤ CVE-2025-24230	
➤ CVE-2025-24237	
➤ CVE-2025-24238	9.8 CRITICAL
➤ CVE-2025-24243	7.8 HIGH

> CVE-2025-24244	
> CVE-2025-24257	
> CVE-2025-24264	
> CVE-2025-24283	
> CVE-2025-27113	5.3 MEDIUM
> CVE-2025-30425	
> CVE-2025-30426	9.8 CRITICAL
> CVE-2025-30427	9.8 CRITICAL
> CVE-2025-30428	
> CVE-2025-30429	
> CVE-2025-30430	
> CVE-2025-30432	
> CVE-2025-30433	
> CVE-2025-30434	
> CVE-2025-30438	
> CVE-2025-30439	
> CVE-2025-30447	5.5 MEDIUM
> CVE-2025-30454	
> CVE-2025-30456	
> CVE-2025-30463	
> CVE-2025-30465	
> CVE-2025-30467	
> CVE-2025-30469	

> CVE-2025-30470	5.5 MEDIUM
> CVE-2025-30471	
> CVE-2025-31182	
> CVE-2025-31183	4.8 MEDIUM
> CVE-2025-31184	4.8 MEDIUM
> CVE-2025-31191	4.8 MEDIUM
> CVE-2025-31192	
> CVE-2024-9681	6.3 MEDIUM
> CVE-2024-48958	5.1 MEDIUM
> CVE-2024-54502	6.5 MEDIUM
> CVE-2024-54508	7.5 HIGH
> CVE-2024-54534	
> CVE-2024-54543	
> CVE-2024-56171	8.1 HIGH
> CVE-2025-24085	
> CVE-2025-24095	
> CVE-2025-24097	5.0 MEDIUM
> CVE-2025-24113	
> CVE-2025-24163	5.5 MEDIUM
> CVE-2025-24167	9.8 CRITICAL
> CVE-2025-24173	
> CVE-2025-24178	
> CVE-2025-24180	

> CVE-2025-24182	
> CVE-2025-24190	
> CVE-2025-24192	
> CVE-2025-24193	
> CVE-2025-24194	
> CVE-2025-24198	
> CVE-2025-24200	
> CVE-2025-24201	8.8 HIGH
> CVE-2025-24202	
> CVE-2025-24203	
> CVE-2025-24205	
> CVE-2025-24208	
> CVE-2025-24209	
> CVE-2025-24210	
> CVE-2025-24211	
> CVE-2025-24212	
> CVE-2025-24213	
> CVE-2025-24214	
> CVE-2025-24215	
> CVE-2025-24216	

CWE's

CWE	Beschrijving
> CWE-1025	Comparison Using Wrong Factors
> CWE-697	Incorrect Comparison
> CWE-125	Out-of-bounds Read
> CWE-284	Improper Access Control
> CWE-416	Use After Free
> CWE-476	NULL Pointer Dereference
> CWE-94	Improper Control of Generation of Code ('Code Injection')
> CWE-400	Uncontrolled Resource Consumption
> CWE-863	Incorrect Authorization
> CWE-787	Out-of-bounds Write
> CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
> CWE-20	Improper Input Validation
> CWE-276	Incorrect Default Permissions
> CWE-275	CWE-275
> CWE-770	Allocation of Resources Without Limits or Throttling

Getroffen producten

Apple
iOS
iOS and iPadOS
iPhone OS

Iphone
Os

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.