



NCSC-2026-0266

Kwetsbaarheden verholpen in Apple iOS en iPadOS

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 28-07-2026

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 diverse versies van iOS en iPadOS.

Duiding

Er zijn diverse geheugenbeheerfouten zoals use-after-free, buffer overflows, out-of-bounds reads en writes, integer overflows, race conditions en insufficient input validation opgelost. Deze fouten kunnen leiden tot onverwachte systeem- of applicatie-terminaties, geheugenbeschadiging, privilege-escalatie, sandbox-ontsnapping, ongeautoriseerde toegang tot gevoelige gebruikersdata, en in sommige gevallen het uitvoeren van willekeurige code. Ook zijn problemen met state management, permissies, sandboxing en UI spoofing in Safari en andere Apple componenten aangepakt. De kwetsbaarheden zijn aanwezig in kerncomponenten van de besturingssystemen en beïnvloeden een breed scala aan Apple-platforms. Exploitatie kan plaatsvinden via speciaal vervaardigde bestanden, netwerkverkeer, webcontent of applicaties. Er zijn geen specifieke proof-of-concept details in de input vermeld.

Oplossingen

Apple heeft updates uitgebracht voor iOS en iPadOS om deze kwetsbaarheden te verhelpen. Gebruikers en beheerders wordt geadviseerd deze updates te installeren om de beveiliging van hun systemen te waarborgen. Zie bijgevoegde referenties voor meer informatie.

Referenties

➤ <https://support.apple.com/en-us/128066>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-3783	6.3 MEDIUM
➤ CVE-2026-3784	6.3 MEDIUM
➤ CVE-2026-4424	6.9 MEDIUM
➤ CVE-2026-28928	
➤ CVE-2026-28931	

> CVE-2026-28973	
> CVE-2026-43673	
> CVE-2026-43711	
> CVE-2026-43714	
> CVE-2026-43723	7.8 HIGH
> CVE-2026-43729	
> CVE-2026-43730	
> CVE-2026-43733	
> CVE-2026-43739	
> CVE-2026-43740	5.3 MEDIUM
> CVE-2026-43744	
> CVE-2026-43753	
> CVE-2026-43769	
> CVE-2026-43776	7.8 HIGH
> CVE-2026-43778	
> CVE-2026-43780	
> CVE-2026-43796	
> CVE-2026-43797	
> CVE-2026-43799	
> CVE-2026-43800	
> CVE-2026-43801	
> CVE-2026-43803	
> CVE-2026-43804	

➤ CVE-2026-43805
➤ CVE-2026-43810
➤ CVE-2026-43811
➤ CVE-2026-43812
➤ CVE-2026-43813
➤ CVE-2026-43814
➤ CVE-2026-43816
➤ CVE-2026-43817
➤ CVE-2026-43818
➤ CVE-2026-43821
➤ CVE-2026-43822
➤ CVE-2026-64692
➤ CVE-2026-64693
➤ CVE-2026-64700
➤ CVE-2026-64707
➤ CVE-2026-64709
➤ CVE-2026-64711
➤ CVE-2026-64713
➤ CVE-2026-64716
➤ CVE-2026-64718
➤ CVE-2026-64719
➤ CVE-2026-64720
➤ CVE-2026-64721

> CVE-2026-64722	
> CVE-2026-64724	
> CVE-2026-64725	
> CVE-2026-64726	
> CVE-2026-64728	
> CVE-2026-64729	
> CVE-2026-64730	
> CVE-2026-64732	
> CVE-2026-64733	
> CVE-2026-64734	
> CVE-2026-64735	
> CVE-2026-64739	
> CVE-2026-64740	
> CVE-2026-64741	
> CVE-2026-64742	
> CVE-2026-64743	
> CVE-2026-64746	
> CVE-2026-64747	
> CVE-2026-64749	
> CVE-2026-64751	
> CVE-2026-64754	
> CVE-2026-64755	4.8 MEDIUM
> CVE-2026-64757	

> CVE-2026-64758	9.4 CRITICAL
> CVE-2026-64763	10.0 CRITICAL
> CVE-2026-64764	9.4 CRITICAL
> CVE-2026-64765	9.4 CRITICAL
> CVE-2026-64766	9.4 CRITICAL
> CVE-2026-64768	5.3 MEDIUM
> CVE-2026-64769	9.4 CRITICAL
> CVE-2026-64770	9.4 CRITICAL
> CVE-2026-64771	9.4 CRITICAL
> CVE-2026-64772	9.4 CRITICAL
> CVE-2026-64774	9.4 CRITICAL
> CVE-2026-64775	6.8 MEDIUM
> CVE-2026-64783	5.3 MEDIUM

CWE's

CWE	Beschrijving
> CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
> CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
> CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
> CWE-125	Out-of-bounds Read
> CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
> CWE-201	Insertion of Sensitive Information Into Sent Data
> CWE-305	Authentication Bypass by Primary Weakness

➤ CWE-416	Use After Free
➤ CWE-522	Insufficiently Protected Credentials

Getroffen producten

Apple
iOS
iPadOS

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.