



# NCSC-2026-0138

## Kwetsbaarheden verholpen in Apple iOS en iPadOS

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 12-05-2026

**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](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 meerdere kwetsbaarheden verholpen in diverse versies van iOS en iPadOS

## Duiding

De kwetsbaarheden betreffen onder andere onjuiste geheugenbeheermechanismen zoals use-after-free, buffer overflows, out-of-bounds reads en writes, race conditions, type confusion, null pointer dereferences, en onvoldoende inputvalidatie. Deze kunnen leiden tot onverwachte applicatie- of systeemcrashes, denial-of-service, ongeautoriseerde toegang tot gevoelige gebruikers- of kerneldata, privilege-escalatie, en het omzeilen van beveiligingsmechanismen zoals Content Security Policy en sandboxing. Sommige kwetsbaarheden maken het mogelijk dat een aanvaller code met kernel-privileges uitvoert of systeemstabiliteit verstoort. De problemen kunnen worden geactiveerd door het verwerken van speciaal vervaardigde bestanden, webcontent, of netwerkverkeer. De fixes omvatten verbeterde validatie, strengere toegangscontroles, en verbeterde geheugen- en state managementmechanismen.

## Oplossingen

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

## Referenties

- <https://support.apple.com/en-us/127110>
- <https://support.apple.com/en-us/127111>
- <https://support.apple.com/en-us/127112>
- <https://support.apple.com/en-us/127113>
- <https://support.apple.com/en-us/127114>

## Kwetsbaarheden

CVE	CVSS Score
➤ <a href="#">CVE-2026-1837</a>	8.7 HIGH
➤ <a href="#">CVE-2026-28819</a>	
➤ <a href="#">CVE-2026-28846</a>	

> CVE-2026-28847	
> CVE-2026-28870	4.8 MEDIUM
> CVE-2026-28872	
> CVE-2026-28873	
> CVE-2026-28877	4.8 MEDIUM
> CVE-2026-28882	4.8 MEDIUM
> CVE-2026-28883	
> CVE-2026-28894	8.7 HIGH
> CVE-2026-28897	
> CVE-2026-28901	
> CVE-2026-28902	
> CVE-2026-28903	
> CVE-2026-28904	
> CVE-2026-28905	
> CVE-2026-28906	
> CVE-2026-28907	
> CVE-2026-28913	
> CVE-2026-28917	
> CVE-2026-28918	
> CVE-2026-28920	
> CVE-2026-28929	
> CVE-2026-28936	
> CVE-2026-28940	

> CVE-2026-28941	
> CVE-2026-28942	
> CVE-2026-28943	
> CVE-2026-28944	
> CVE-2026-28947	
> CVE-2026-28950	6.2 MEDIUM
> CVE-2026-28951	
> CVE-2026-28952	
> CVE-2026-28953	
> CVE-2026-28954	
> CVE-2026-28955	
> CVE-2026-28956	
> CVE-2026-28957	
> CVE-2026-28958	
> CVE-2026-28959	
> CVE-2026-28962	
> CVE-2026-28963	
> CVE-2026-28964	
> CVE-2026-28965	
> CVE-2026-28969	
> CVE-2026-28971	
> CVE-2026-28972	
> CVE-2026-28974	

> [CVE-2026-28977](#)

> [CVE-2026-28983](#)

> [CVE-2026-28985](#)

> [CVE-2026-28986](#)

> [CVE-2026-28987](#)

> [CVE-2026-28988](#)

> [CVE-2026-28990](#)

> [CVE-2026-28991](#)

> [CVE-2026-28992](#)

> [CVE-2026-28993](#)

> [CVE-2026-28994](#)

> [CVE-2026-28995](#)

> [CVE-2026-28996](#)

> [CVE-2026-39869](#)

> [CVE-2026-43653](#)

> [CVE-2026-43654](#)

> [CVE-2026-43655](#)

> [CVE-2026-43656](#)

> [CVE-2026-43658](#)

> [CVE-2026-43659](#)

> [CVE-2026-43660](#)

> [CVE-2026-43661](#)

> [CVE-2026-43666](#)

[> CVE-2026-43668](#)

## CWE's

CWE	Beschrijving
<a href="#">&gt; CWE-20</a>	Improper Input Validation
<a href="#">&gt; CWE-200</a>	Exposure of Sensitive Information to an Unauthorized Actor
<a href="#">&gt; CWE-359</a>	Exposure of Private Personal Information to an Unauthorized Actor
<a href="#">&gt; CWE-404</a>	Improper Resource Shutdown or Release
<a href="#">&gt; CWE-770</a>	Allocation of Resources Without Limits or Throttling
<a href="#">&gt; CWE-787</a>	Out-of-bounds Write
<a href="#">&gt; CWE-805</a>	Buffer Access with Incorrect Length Value

## 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.