Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0370

Kwetsbaarheden verholpen in Apple iOS en iPadOS

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 15-09-2026

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 iOS en iPadOS.

Duiding

De kwetsbaarheden betreffen diverse beveiligingsproblemen zoals authenticatiefouten, out-of-bounds schrijf- en leesfouten, use-after-free, buffer overflows, race conditions, permissie- en autorisatieproblemen, geheugenbeschadiging, informatielekken, logica- en validatiefouten, en privacy-gerelateerde zwakheden. Aanvallers kunnen deze kwetsbaarheden misbruiken om ongeautoriseerde toegang te verkrijgen tot gebruikersgegevens, systeeminstabiliteit te veroorzaken door onverwachte systeem- of applicatieafsluitingen, kernelgeheugen te lezen of te beschadigen, privileges te escaleren, sandbox-beperkingen te omzeilen, en netwerkverkeer te manipuleren. Sommige kwetsbaarheden kunnen leiden tot het uitlekken van gevoelige informatie zoals Wi-Fi-wachtwoorden, apparaatidentificatoren, en gebruikerslocaties. De problemen zijn aanwezig in kerncomponenten van de besturingssystemen en diverse subsysteemfuncties zoals bestandshandling, geheugenbeheer, authenticatieprocessen, en webcontentverwerking. De fixes zijn doorgevoerd via verbeterde validatie, strengere toegangscontroles, verbeterde geheugen- en state management, en het verwijderen van kwetsbare code.

Oplossingen

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

Referenties

- https://support.apple.com/en-us/149034
- https://support.apple.com/en-us/149041

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-20683	
CVE-2026-28966	
CVE-2026-28968	
CVE-2026-28969	7.5 HIGH

CVE-2026-43661	7.5 HIGH
CVE-2026-43664	
CVE-2026-43674	
CVE-2026-43684	
CVE-2026-43686	8.8 HIGH
CVE-2026-43687	6.5 MEDIUM
CVE-2026-43688	
CVE-2026-43689	7.8 HIGH
CVE-2026-43695	
CVE-2026-43702	
CVE-2026-43715	8.8 HIGH
CVE-2026-43737	
CVE-2026-43738	5.5 MEDIUM
CVE-2026-43743	4.7 MEDIUM
CVE-2026-43785	
CVE-2026-64718	5.5 MEDIUM
CVE-2026-64752	7.3 HIGH
CVE-2026-64753	6.5 MEDIUM
CVE-2026-64756	
CVE-2026-64758	7.8 HIGH
CVE-2026-64760	5.5 MEDIUM
CVE-2026-64761	
CVE-2026-65329	5.9 MEDIUM

CVE-2026-65344	
CVE-2026-65345	
CVE-2026-65348	
CVE-2026-65354	
CVE-2026-65358	
CVE-2026-65359	
CVE-2026-65360	
CVE-2026-65377	
CVE-2026-65395	6.5 MEDIUM
CVE-2026-65398	
CVE-2026-65399	
CVE-2026-65402	
CVE-2026-65403	
CVE-2026-65404	
CVE-2026-65405	
CVE-2026-65406	
CVE-2026-65407	
CVE-2026-65408	
CVE-2026-65409	
CVE-2026-65410	
CVE-2026-65411	
CVE-2026-65412	
CVE-2026-65414	9.8 CRITICAL

CVE-2026-65415	8.1 HIGH
CVE-2026-84487	
CVE-2026-84489	5.5 MEDIUM
CVE-2026-84491	
CVE-2026-84492	4.7 MEDIUM
CVE-2026-84497	
CVE-2026-84507	
CVE-2026-84510	
CVE-2026-84511	
CVE-2026-84513	
CVE-2026-84518	4.3 MEDIUM
CVE-2026-84519	6.5 MEDIUM
CVE-2026-84521	
CVE-2026-84523	5.5 MEDIUM
CVE-2026-84524	
CVE-2026-84526	
CVE-2026-84527	
CVE-2026-84530	
CVE-2026-84531	
CVE-2026-84532	
CVE-2026-84533	
CVE-2026-84534	
CVE-2026-84546	

CVE-2026-84551	
CVE-2026-84552	
CVE-2026-84560	
CVE-2026-84561	
CVE-2026-84564	
CVE-2026-84566	
CVE-2026-84571	
CVE-2026-84575	
CVE-2026-84583	
CVE-2026-84593	
CVE-2026-84596	6.5 MEDIUM
CVE-2026-84597	6.5 MEDIUM
CVE-2026-84598	
CVE-2026-84600	
CVE-2026-84602	
CVE-2026-84603	
CVE-2026-84606	
CVE-2026-84607	7.8 HIGH
CVE-2026-84609	
CVE-2026-84611	7.3 HIGH
CVE-2026-84612	
CVE-2026-84615	
CVE-2026-84616	

CVE-2026-84617	5.5 MEDIUM
CVE-2026-84620	
CVE-2026-84621	
CVE-2026-84622	
CVE-2026-84623	
CVE-2026-84624	
CVE-2026-84625	
CVE-2026-84626	
CVE-2026-84628	
CVE-2026-84629	
CVE-2026-84630	4.7 MEDIUM
CVE-2026-84632	
CVE-2026-84635	
CVE-2026-84636	
CVE-2026-86869	
CVE-2026-86870	
CVE-2026-86876	5.2 MEDIUM
CVE-2026-86878	
CVE-2026-86879	6.5 MEDIUM
CVE-2026-86881	
CVE-2026-86882	6.5 MEDIUM
CVE-2026-86883	
CVE-2026-86884	

CVE-2026-86885	**6.5 MEDIUM**
CVE-2026-86886	
CVE-2026-86887	
CVE-2026-86888	
CVE-2026-86890	
CVE-2026-86892	
CVE-2026-86893	
CVE-2026-86895	
CVE-2026-86897	
CVE-2026-86898	
CVE-2026-86903	**5.5 MEDIUM**
CVE-2026-86904	
CVE-2026-86905	**5.5 MEDIUM**
CVE-2026-86924	

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-121	Stack-based Buffer Overflow
CWE-125	Out-of-bounds Read
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

CWE-404	Improper Resource Shutdown or Release
CWE-416	Use After Free
CWE-642	External Control of Critical State Data
CWE-787	Out-of-bounds Write
CWE-862	Missing Authorization

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.