Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0319

Kwetsbaarheden verholpen in Apple iOS en iPadOS

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 20-08-2026

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 onder andere onjuist geheugenbeheer zoals use-after-free, buffer overflows, out-of-bounds reads en writes, integer overflows, race conditions, en onvoldoende inputvalidatie. Deze fouten kunnen leiden tot onverwachte crashes, geheugenbeschadiging, het lekken van gevoelige gegevens zoals OAuth2 tokens en kernel geheugen, het omzeilen van sandboxbeperkingen, en in sommige gevallen het uitvoeren van arbitraire code. Bij libcurl kunnen OAuth2 bearer tokens bijvoorbeeld gelekt worden naar een tweede host tijdens HTTP(S) redirects in combinatie met .netrc bestand gebruik. In WebKitGTK kunnen kwaadaardig opgemaakte webcontent en bestanden leiden tot procescrashes, sandbox escapes, en datalekken. Diverse Apple besturingssystemen zijn getroffen door kwetsbaarheden die het mogelijk maken dat applicaties zonder juiste autorisatie toegang krijgen tot gevoelige gebruikersdata, contactinformatie, of systeembronnen. Er zijn ook problemen opgelost die het mogelijk maakten dat applicaties bestanden buiten hun sandbox konden lezen of verwijderen. De updates verbeteren de validatie van invoer, geheugenbeheer, en beveiligingscontroles om deze risico's te mitigeren.

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/148287
- https://support.apple.com/en-us/148282

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-3783	5.7 MEDIUM
CVE-2026-3784	6.5 MEDIUM
CVE-2026-4424	7.5 HIGH
CVE-2026-28947	8.8 HIGH

CVE-2026-28958	6.5 MEDIUM
CVE-2026-28973	8.6 HIGH
CVE-2026-28979	6.5 MEDIUM
CVE-2026-28984	4.3 MEDIUM
CVE-2026-28990	7.5 HIGH
CVE-2026-28996	5.5 MEDIUM
CVE-2026-39868	9.1 CRITICAL
CVE-2026-39872	6.5 MEDIUM
CVE-2026-39877	7.8 HIGH
CVE-2026-43658	8.8 HIGH
CVE-2026-43661	7.5 HIGH
CVE-2026-43663	6.5 MEDIUM
CVE-2026-43667	6.5 MEDIUM
CVE-2026-43673	7.8 HIGH
CVE-2026-43676	6.5 MEDIUM
CVE-2026-43699	6.5 MEDIUM
CVE-2026-43700	6.5 MEDIUM
CVE-2026-43701	7.1 HIGH
CVE-2026-43705	8.8 HIGH
CVE-2026-43708	4.3 MEDIUM
CVE-2026-43711	7.8 HIGH
CVE-2026-43714	5.5 MEDIUM
CVE-2026-43717	6.5 MEDIUM

CVE-2026-43720	6.5 MEDIUM
CVE-2026-43722	5.5 MEDIUM
CVE-2026-43723	7.8 HIGH
CVE-2026-43724	7.8 HIGH
CVE-2026-43725	7.1 HIGH
CVE-2026-43726	6.5 MEDIUM
CVE-2026-43727	6.5 MEDIUM
CVE-2026-43729	7.8 HIGH
CVE-2026-43731	8.8 HIGH
CVE-2026-43733	7.8 HIGH
CVE-2026-43734	6.5 MEDIUM
CVE-2026-43735	8.1 HIGH
CVE-2026-43738	5.5 MEDIUM
CVE-2026-43742	6.5 MEDIUM
CVE-2026-43744	5.5 MEDIUM
CVE-2026-43745	6.5 MEDIUM
CVE-2026-43754	5.5 MEDIUM
CVE-2026-43757	9.8 CRITICAL
CVE-2026-43769	9.8 CRITICAL
CVE-2026-43776	7.8 HIGH
CVE-2026-43778	9.8 CRITICAL
CVE-2026-43794	8.8 HIGH
CVE-2026-43795	4.3 MEDIUM

CVE-2026-43796	5.5 MEDIUM
CVE-2026-43797	5.5 MEDIUM
CVE-2026-43799	9.8 CRITICAL
CVE-2026-43800	5.5 MEDIUM
CVE-2026-43801	5.5 MEDIUM
CVE-2026-43802	9.8 CRITICAL
CVE-2026-43803	9.8 CRITICAL
CVE-2026-43807	9.8 CRITICAL
CVE-2026-43809	9.8 CRITICAL
CVE-2026-43810	9.8 CRITICAL
CVE-2026-43811	4.7 MEDIUM
CVE-2026-43812	9.8 CRITICAL
CVE-2026-43818	8.8 HIGH
CVE-2026-43821	6.5 MEDIUM
CVE-2026-43822	9.8 CRITICAL
CVE-2026-64692	7.1 HIGH
CVE-2026-64693	5.5 MEDIUM
CVE-2026-64695	9.8 CRITICAL
CVE-2026-64700	9.8 CRITICAL
CVE-2026-64707	5.5 MEDIUM
CVE-2026-64709	5.5 MEDIUM
CVE-2026-64715	6.5 MEDIUM
CVE-2026-64716	7.8 HIGH

CVE-2026-64719	8.1 HIGH
CVE-2026-64721	5.5 MEDIUM
CVE-2026-64722	5.5 MEDIUM
CVE-2026-64723	5.5 MEDIUM
CVE-2026-64724	5.5 MEDIUM
CVE-2026-64725	7.1 HIGH
CVE-2026-64726	9.8 CRITICAL
CVE-2026-64732	4.6 MEDIUM
CVE-2026-64734	5.5 MEDIUM
CVE-2026-64735	6.5 MEDIUM
CVE-2026-64738	9.8 CRITICAL
CVE-2026-64739	8.8 HIGH
CVE-2026-64740	9.3 CRITICAL
CVE-2026-64742	6.5 MEDIUM
CVE-2026-64743	6.5 MEDIUM
CVE-2026-64744	5.5 MEDIUM
CVE-2026-64746	9.8 CRITICAL
CVE-2026-64747	7.8 HIGH
CVE-2026-64749	7.8 HIGH
CVE-2026-64755	5.5 MEDIUM
CVE-2026-64757	8.8 HIGH
CVE-2026-64760	5.5 MEDIUM
CVE-2026-64762	9.8 CRITICAL

CVE-2026-64763	7.8 HIGH
CVE-2026-64764	7.8 HIGH
CVE-2026-64765	7.8 HIGH
CVE-2026-64766	7.8 HIGH
CVE-2026-64768	8.1 HIGH
CVE-2026-64769	9.8 CRITICAL
CVE-2026-64770	9.8 CRITICAL
CVE-2026-64771	9.8 CRITICAL
CVE-2026-64772	9.8 CRITICAL
CVE-2026-64774	9.8 CRITICAL
CVE-2026-64778	6.5 MEDIUM
CVE-2026-64779	3.1 LOW
CVE-2026-64780	4.3 MEDIUM
CVE-2026-64781	4.3 MEDIUM
CVE-2026-64782	3.1 LOW
CVE-2026-64784	4.3 MEDIUM
CVE-2026-65331	4.3 MEDIUM
CVE-2026-65332	4.3 MEDIUM
CVE-2026-65333	4.3 MEDIUM
CVE-2026-65334	4.3 MEDIUM
CVE-2026-65335	4.3 MEDIUM
CVE-2026-65336	4.3 MEDIUM
CVE-2026-65337	4.3 MEDIUM

CVE-2026-65338	**4.3 MEDIUM**
CVE-2026-65340	**4.3 MEDIUM**
CVE-2026-65341	**5.4 MEDIUM**

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
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-121	Stack-based Buffer Overflow
CWE-125	Out-of-bounds Read
CWE-190	Integer Overflow or Wraparound
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-201	Insertion of Sensitive Information Into Sent Data
CWE-265	Privilege Issues
CWE-284	Improper Access Control
CWE-285	Improper Authorization
CWE-305	Authentication Bypass by Primary Weakness
CWE-319	Cleartext Transmission of Sensitive Information
CWE-346	Origin Validation Error
CWE-352	Cross-Site Request Forgery (CSRF)
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-400	Uncontrolled Resource Consumption

CWE-404	Improper Resource Shutdown or Release
CWE-416	Use After Free
CWE-451	User Interface (UI) Misrepresentation of Critical Information
CWE-522	Insufficiently Protected Credentials
CWE-617	Reachable Assertion
CWE-664	Improper Control of a Resource Through its Lifetime
CWE-703	Improper Check or Handling of Exceptional Conditions
CWE-732	Incorrect Permission Assignment for Critical Resource
CWE-787	Out-of-bounds Write
CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')
CWE-862	Missing Authorization
CWE-942	Permissive Cross-domain Security Policy with Untrusted Domains

Getroffen producten

Apple
iOS
iPadOS

Disclaimer