Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0317

Kwetsbaarheden verholpen in Apple macOS

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 kwetsbaarheden verholpen in macOS Tahoe 26.6.2

Duiding

De kwetsbaarheden betreffen meerdere aspecten van geheugenbeheer, inputvalidatie en state management binnen Apple's besturingssystemen en Safari-browser. Een aantal kwetsbaarheden maakt het mogelijk dat een kwaadwillende door het verwerken van speciaal vervaardigde webcontent of afbeeldingen geheugenbeschadiging veroorzaakt, wat kan leiden tot onverwachte crashes, systeemterminatie of het lekken van gevoelige gebruikersinformatie. Andere kwetsbaarheden betreffen use-after-free-condities en out-of-bounds memory access, die eveneens kunnen resulteren in systeeminstabiliteit of het blootstellen van kernelgeheugen. De problemen zijn aanwezig in de mechanismen die app-toegang tot gebruikersdata controleren, de verwerking van webcontent en de afhandeling van afbeeldingen. Door verbeterde validatie, geheugenbeheer en lockingmechanismen toe te passen, voorkomt Apple dat deze kwetsbaarheden kunnen worden misbruikt om crashes, denial-of-service of ongeautoriseerde informatie-expositie te veroorzaken.

Oplossingen

Apple heeft updates uitgebracht voor macOS Tahoe 26.6.2 die verbeterde controles, geheugenbeheer en validatiemechanismen implementeren om de beschreven kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://support.apple.com/en-us/148281

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-65339	5.0 MEDIUM
CVE-2026-65347	6.5 MEDIUM
CVE-2026-65346	8.8 HIGH
CVE-2026-64788	5.4 MEDIUM
CVE-2026-65343	7.5 HIGH

CVE-2026-65349	6.6 MEDIUM
CVE-2026-65330	6.5 MEDIUM
CVE-2026-64784	4.3 MEDIUM
CVE-2026-43795	4.3 MEDIUM
CVE-2026-65338	4.3 MEDIUM
CVE-2026-65341	5.4 MEDIUM
CVE-2026-64782	3.1 LOW
CVE-2026-64781	4.3 MEDIUM
CVE-2026-65351	4.3 MEDIUM
CVE-2026-65340	4.3 MEDIUM
CVE-2026-65337	4.3 MEDIUM
CVE-2026-65336	4.3 MEDIUM
CVE-2026-65335	4.3 MEDIUM
CVE-2026-65333	4.3 MEDIUM
CVE-2026-65332	4.3 MEDIUM
CVE-2026-65331	4.3 MEDIUM
CVE-2026-64715	6.5 MEDIUM
CVE-2026-64780	4.3 MEDIUM
CVE-2026-65334	4.3 MEDIUM
CVE-2026-43794	8.8 HIGH
CVE-2026-64787	6.5 MEDIUM
CVE-2026-64778	6.5 MEDIUM
CVE-2026-64779	3.1 LOW

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
CWE-125	Out-of-bounds Read
CWE-190	Integer Overflow or Wraparound
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-269	Improper Privilege Management
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-693	Protection Mechanism Failure
CWE-703	Improper Check or Handling of Exceptional Conditions
CWE-787	Out-of-bounds Write

Getroffen producten

Apple
macOS Tahoe

Disclaimer