



NCSC-2026-0214

Kwetsbaarheden verholpen in Apple MacOS

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 30-06-2026

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 macOS Tahoe.

Duiding

De kwetsbaarheden betroffen onder andere out-of-bounds access, use-after-free, memory handling fouten, type confusion, double free, stack overflow, insufficient input validation, en race conditions. Deze konden leiden tot onverwachte crashes van processen, corruptie van geheugen, ongeautoriseerde toegang tot gevoelige data zoals clipboard-inhoud en kernelinformatie, en het omzeilen van sandbox-beperkingen. Kwaadwillenden kunnen deze kwetsbaarheden misbruiken door speciaal vervaardigde webcontent of applicaties aan te bieden die de genoemde fouten triggeren, wat resulteert in procesinstabiliteit, systeemterminatie of datalekken. De kwetsbaarheden zijn opgelost door verbeterde bounds checking, input validatie, geheugenbeheer, state management en synchronisatie.

Oplossingen

Apple heeft updates uitgebracht voor macOS Tahoe 26.5.2 om deze kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

➤ <https://support.apple.com/en-us/127595>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-28979	6.5 MEDIUM
➤ CVE-2026-39868	
➤ CVE-2026-39872	6.5 MEDIUM
➤ CVE-2026-43663	6.5 MEDIUM
➤ CVE-2026-43676	6.5 MEDIUM
➤ CVE-2026-43699	6.5 MEDIUM

> CVE-2026-43700	6.5 MEDIUM
> CVE-2026-43701	
> CVE-2026-43703	6.5 MEDIUM
> CVE-2026-43704	5.3 MEDIUM
> CVE-2026-43705	8.8 HIGH
> CVE-2026-43706	6.5 MEDIUM
> CVE-2026-43707	
> CVE-2026-43708	4.3 MEDIUM
> CVE-2026-43709	6.5 MEDIUM
> CVE-2026-43712	6.5 MEDIUM
> CVE-2026-43713	
> CVE-2026-43715	8.8 HIGH
> CVE-2026-43716	6.5 MEDIUM
> CVE-2026-43717	6.5 MEDIUM
> CVE-2026-43718	5.3 MEDIUM
> CVE-2026-43720	5.3 MEDIUM
> CVE-2026-43721	5.3 MEDIUM
> CVE-2026-43722	4.8 MEDIUM
> CVE-2026-43724	4.8 MEDIUM
> CVE-2026-43725	5.3 MEDIUM
> CVE-2026-43726	5.3 MEDIUM
> CVE-2026-43727	5.3 MEDIUM
> CVE-2026-43731	5.3 MEDIUM

> CVE-2026-43732	5.3 MEDIUM
> CVE-2026-43734	5.3 MEDIUM
> CVE-2026-43735	5.3 MEDIUM
> CVE-2026-43740	5.3 MEDIUM
> CVE-2026-43742	5.3 MEDIUM
> CVE-2026-43743	2.0 LOW
> CVE-2026-43745	5.3 MEDIUM
> CVE-2026-43746	5.3 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-121	Stack-based Buffer Overflow
> CWE-125	Out-of-bounds Read
> CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
> CWE-265	Privilege Issues
> CWE-346	Origin Validation Error
> CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
> CWE-404	Improper Resource Shutdown or Release
> CWE-415	Double Free
> CWE-416	Use After Free

➤ CWE-787	Out-of-bounds Write
➤ CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')
➤ CWE-942	Permissive Cross-domain Security Policy with Untrusted Domains

Getroffen producten

Apple
macOS Tahoe

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.