



# NCSC-2025-0396

## Kwetsbaarheden verholpen in Apple macOS

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 15-12-2025

**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 kwetsbaarheden verholpen in macOS Sonoma (14.8.3), macOS Sequoia (15.7.3) en macOS Tahoe (26.2).

## Duiding

De kwetsbaarheden omvatten een breed scala aan problemen, waaronder geheugenbeschadiging, logboekproblemen, en ongeoorloofde toegang tot gevoelige gebruikersgegevens. Deze kwetsbaarheden konden worden misbruikt door kwaadwillenden om ongeautoriseerde toegang te verkrijgen of om de stabiliteit van het systeem in gevaar te brengen.

Voor succesvol misbruik moet de kwaadwillende het slachtoffer misleiden een malafide app te installeren of bestand te openen.

## Oplossingen

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

## Referenties

- <https://support.apple.com/en-us/125886>
- <https://support.apple.com/en-us/125887>
- <https://support.apple.com/en-us/125888>

## Kwetsbaarheden

CVE	CVSS Score
➤ <a href="#">CVE-2024-7264</a>	5.1 MEDIUM
➤ <a href="#">CVE-2024-8906</a>	4.3 MEDIUM
➤ <a href="#">CVE-2025-5918</a>	5.3 MEDIUM
➤ <a href="#">CVE-2025-9086</a>	2.3 LOW
➤ <a href="#">CVE-2025-14174</a>	8.8 HIGH
➤ <a href="#">CVE-2025-43320</a>	

> CVE-2025-43410	2.4 LOW
> CVE-2025-43416	4.8 MEDIUM
> CVE-2025-43428	
> CVE-2025-43463	4.8 MEDIUM
> CVE-2025-43482	4.8 MEDIUM
> CVE-2025-43501	
> CVE-2025-43509	4.8 MEDIUM
> CVE-2025-43511	5.3 MEDIUM
> CVE-2025-43512	4.8 MEDIUM
> CVE-2025-43513	4.8 MEDIUM
> CVE-2025-43514	
> CVE-2025-43516	4.8 MEDIUM
> CVE-2025-43517	4.8 MEDIUM
> CVE-2025-43518	4.8 MEDIUM
> CVE-2025-43519	4.8 MEDIUM
> CVE-2025-43521	4.8 MEDIUM
> CVE-2025-43522	4.8 MEDIUM
> CVE-2025-43523	4.8 MEDIUM
> CVE-2025-43526	
> CVE-2025-43527	8.5 HIGH
> CVE-2025-43529	
> CVE-2025-43530	4.8 MEDIUM
> CVE-2025-43531	

> CVE-2025-43532	6.9 MEDIUM
> CVE-2025-43533	
> CVE-2025-43535	
> CVE-2025-43536	
> CVE-2025-43538	4.8 MEDIUM
> CVE-2025-43539	5.3 MEDIUM
> CVE-2025-43541	
> CVE-2025-43542	5.3 MEDIUM
> CVE-2025-46276	4.8 MEDIUM
> CVE-2025-46277	
> CVE-2025-46278	
> CVE-2025-46279	
> CVE-2025-46281	
> CVE-2025-46282	
> CVE-2025-46283	
> CVE-2025-46285	8.5 HIGH
> CVE-2025-46287	5.3 MEDIUM
> CVE-2025-46288	
> CVE-2025-46289	4.8 MEDIUM
> CVE-2025-46291	

## CWE's

CWE	Beschrijving
> CWE-20	Improper Input Validation
> 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-125	Out-of-bounds Read
> CWE-190	Integer Overflow or Wraparound
> CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
> CWE-275	CWE-275
> CWE-280	Improper Handling of Insufficient Permissions or Privileges
> CWE-284	Improper Access Control
> CWE-359	Exposure of Private Personal Information to an Unauthorized Actor
> CWE-371	CWE-371
> CWE-404	Improper Resource Shutdown or Release
> CWE-416	Use After Free
> CWE-451	User Interface (UI) Misrepresentation of Critical Information
> CWE-456	Missing Initialization of a Variable
> CWE-488	Exposure of Data Element to Wrong Session
> CWE-524	Use of Cache Containing Sensitive Information
> CWE-532	Insertion of Sensitive Information into Log File
> CWE-732	Incorrect Permission Assignment for Critical Resource
> CWE-862	Missing Authorization
> CWE-1018	CWE-1018

## Getroffen producten

<b>Apple</b>
macOS Sequoia
macOS Sonoma
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.