



NCSC-2025-0351

Kwetsbaarheden verholpen in Apple MacOS

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 04-11-2025

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).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Apple heeft kwetsbaarheden verholpen in macOS Sonoma 14.8.2, macOS Sequoia 15.7.2 en MacOS Tahoe 26.1.

Duiding

De kwetsbaarheden omvatten een breed scala aan problemen, waaronder ongeautoriseerde toegang tot gevoelige gebruikersdata, racecondities, en logische fouten die konden leiden tot ongewenste toegang of systeeminstabiliteit. Aanvallers konden deze kwetsbaarheden misbruiken door gebruik te maken van onjuiste validatieprocessen en beveiligingslekken in de sandbox-omgeving. De impact varieerde van gegevenslekken tot potentiële systeemcrashes, wat de noodzaak van onmiddellijke aandacht benadrukte.

Oplossingen

Apple heeft updates uitgebracht om de kwetsbaarheden te verhelpen, waaronder verbeterde validatieprocessen, extra restricties in de sandbox-omgeving, en verbeteringen in het geheugenbeheer. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://support.apple.com/en-us/125634>
- <https://support.apple.com/en-us/125635>
- <https://support.apple.com/en-us/125636>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2024-43398	8.2 HIGH
➤ CVE-2024-49761	8.7 HIGH
➤ CVE-2025-6442	6.3 MEDIUM
➤ CVE-2025-30465	9.8 CRITICAL
➤ CVE-2025-31199	5.5 MEDIUM
➤ CVE-2025-32462	7.3 HIGH

> CVE-2025-43292	2.0 LOW
> CVE-2025-43322	
> CVE-2025-43334	
> CVE-2025-43335	
> CVE-2025-43336	
> CVE-2025-43337	4.8 MEDIUM
> CVE-2025-43338	
> CVE-2025-43348	
> CVE-2025-43351	
> CVE-2025-43361	
> CVE-2025-43364	
> CVE-2025-43372	5.3 MEDIUM
> CVE-2025-43373	
> CVE-2025-43377	
> CVE-2025-43378	
> CVE-2025-43379	
> CVE-2025-43380	
> CVE-2025-43381	
> CVE-2025-43382	
> CVE-2025-43383	
> CVE-2025-43384	
> CVE-2025-43385	
> CVE-2025-43386	

> CVE-2025-43387	
> CVE-2025-43388	
> CVE-2025-43389	
> CVE-2025-43390	
> CVE-2025-43391	
> CVE-2025-43392	
> CVE-2025-43393	
> CVE-2025-43394	4.8 MEDIUM
> CVE-2025-43395	4.8 MEDIUM
> CVE-2025-43396	4.8 MEDIUM
> CVE-2025-43397	6.8 MEDIUM
> CVE-2025-43398	6.8 MEDIUM
> CVE-2025-43399	4.8 MEDIUM
> CVE-2025-43401	
> CVE-2025-43402	
> CVE-2025-43404	
> CVE-2025-43405	4.8 MEDIUM
> CVE-2025-43406	
> CVE-2025-43407	4.8 MEDIUM
> CVE-2025-43408	2.4 LOW
> CVE-2025-43409	4.8 MEDIUM
> CVE-2025-43411	4.8 MEDIUM
> CVE-2025-43412	4.8 MEDIUM

> CVE-2025-43413	2.1 LOW
> CVE-2025-43414	
> CVE-2025-43420	2.0 LOW
> CVE-2025-43421	
> CVE-2025-43423	2.4 LOW
> CVE-2025-43424	4.8 MEDIUM
> CVE-2025-43425	
> CVE-2025-43426	4.8 MEDIUM
> CVE-2025-43427	
> CVE-2025-43429	
> CVE-2025-43430	
> CVE-2025-43431	
> CVE-2025-43432	
> CVE-2025-43433	
> CVE-2025-43434	
> CVE-2025-43435	
> CVE-2025-43436	4.8 MEDIUM
> CVE-2025-43438	
> CVE-2025-43440	
> CVE-2025-43441	
> CVE-2025-43443	
> CVE-2025-43444	4.8 MEDIUM
> CVE-2025-43445	5.3 MEDIUM

> CVE-2025-43446	4.8 MEDIUM
> CVE-2025-43447	
> CVE-2025-43448	4.8 MEDIUM
> CVE-2025-43455	4.8 MEDIUM
> CVE-2025-43457	
> CVE-2025-43458	
> CVE-2025-43461	
> CVE-2025-43462	
> CVE-2025-43463	
> CVE-2025-43464	
> CVE-2025-43465	
> CVE-2025-43466	
> CVE-2025-43467	
> CVE-2025-43468	4.8 MEDIUM
> CVE-2025-43469	4.8 MEDIUM
> CVE-2025-43471	
> CVE-2025-43472	8.5 HIGH
> CVE-2025-43473	
> CVE-2025-43474	
> CVE-2025-43476	4.8 MEDIUM
> CVE-2025-43477	4.8 MEDIUM
> CVE-2025-43478	6.8 MEDIUM
> CVE-2025-43479	4.8 MEDIUM

> CVE-2025-43480	
> CVE-2025-43481	4.8 MEDIUM
> CVE-2025-43493	
> CVE-2025-43496	
> CVE-2025-43497	
> CVE-2025-43498	4.8 MEDIUM
> CVE-2025-43499	4.8 MEDIUM
> CVE-2025-43500	4.8 MEDIUM
> CVE-2025-43502	4.8 MEDIUM
> CVE-2025-43503	
> CVE-2025-43506	
> CVE-2025-43507	4.8 MEDIUM
> CVE-2025-53906	2.3 LOW

CWE's

CWE	Beschrijving
> CVE-20	Improper Input Validation
> CVE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
> CVE-61	UNIX Symbolic Link (Symlink) Following
> CVE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
> CVE-125	Out-of-bounds Read
> CVE-200	Exposure of Sensitive Information to an Unauthorized Actor
> CVE-265	CWE-265

➤ CWE-275	CWE-275
➤ CWE-276	Incorrect Default Permissions
➤ CWE-284	Improper Access Control
➤ 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-444	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
➤ CWE-532	Insertion of Sensitive Information into Log File
➤ CWE-776	Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')
➤ CWE-863	Incorrect Authorization
➤ CWE-1333	Inefficient Regular Expression Complexity

Getroffen producten

Apple
Mac OS
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.