Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0371

Kwetsbaarheden verholpen in Apple macOS en Samba door Apple en Samba

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 15-09-2026

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 (Specifiek voor Golden Gate 27, Sequoia 15.8, Tahoe 26.7).

Duiding

De kwetsbaarheden in macOS betreffen onder andere heap-based buffer overflows, use-after-free fouten, integer overflows, null pointer dereferences, onjuiste toegangscontrole, privilege escalatie, race conditions, out-of-bounds reads en writes, loggingsproblemen, en problemen met state management. Deze kunnen leiden tot onverwachte systeem- of applicatie-terminaties, kernel geheugen corruptie, ongeautoriseerde toegang tot gevoelige gebruikersdata, omzeilen van sandbox- en Gatekeeper-beveiligingen, en het mogelijk maken van remote code execution of denial-of-service.

Oplossingen

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

Referenties

- https://support.apple.com/en-us/149035
- https://support.apple.com/en-us/149042
- https://support.apple.com/en-us/149043

Kwetsbaarheden

CVE	CVSS Score
CVE-2022-3437	6.5 MEDIUM
CVE-2026-20683	
CVE-2026-28899	
CVE-2026-28930	7.5 HIGH
CVE-2026-28934	
CVE-2026-28935	

CVE-2026-28937	
CVE-2026-28966	
CVE-2026-28968	
CVE-2026-28969	7.5 HIGH
CVE-2026-34979	5.3 MEDIUM
CVE-2026-43664	
CVE-2026-43677	6.5 MEDIUM
CVE-2026-43683	
CVE-2026-43684	
CVE-2026-43686	8.8 HIGH
CVE-2026-43687	6.5 MEDIUM
CVE-2026-43688	
CVE-2026-43689	7.8 HIGH
CVE-2026-43690	
CVE-2026-43691	7.8 HIGH
CVE-2026-43692	8.8 HIGH
CVE-2026-43695	
CVE-2026-43696	
CVE-2026-43697	
CVE-2026-43698	7.8 HIGH
CVE-2026-43702	
CVE-2026-43719	
CVE-2026-43737	

CVE-2026-43738	5.5 MEDIUM
CVE-2026-43741	
CVE-2026-43743	4.7 MEDIUM
CVE-2026-43760	8.6 HIGH
CVE-2026-43763	5.5 MEDIUM
CVE-2026-43785	
CVE-2026-43786	7.8 HIGH
CVE-2026-43787	
CVE-2026-43788	
CVE-2026-43789	
CVE-2026-43790	
CVE-2026-43791	
CVE-2026-64712	7.8 HIGH
CVE-2026-64714	
CVE-2026-64718	5.5 MEDIUM
CVE-2026-64736	7.1 HIGH
CVE-2026-64752	7.3 HIGH
CVE-2026-64753	6.5 MEDIUM
CVE-2026-64756	
CVE-2026-64758	7.8 HIGH
CVE-2026-64760	5.5 MEDIUM
CVE-2026-64790	
CVE-2026-65330	6.5 MEDIUM

CVE-2026-65339	5.0 MEDIUM
CVE-2026-65342	
CVE-2026-65344	
CVE-2026-65345	
CVE-2026-65346	8.8 HIGH
CVE-2026-65348	
CVE-2026-65349	6.6 MEDIUM
CVE-2026-65354	
CVE-2026-65358	
CVE-2026-65359	
CVE-2026-65360	
CVE-2026-65361	
CVE-2026-65362	7.8 HIGH
CVE-2026-65364	7.5 HIGH
CVE-2026-65365	
CVE-2026-65369	
CVE-2026-65371	
CVE-2026-65374	8.8 HIGH
CVE-2026-65375	
CVE-2026-65376	
CVE-2026-65377	
CVE-2026-65378	
CVE-2026-65380	

CVE-2026-65381	
CVE-2026-65382	
CVE-2026-65383	
CVE-2026-65393	
CVE-2026-65395	6.5 MEDIUM
CVE-2026-65398	
CVE-2026-65399	
CVE-2026-65400	9.8 CRITICAL
CVE-2026-65401	
CVE-2026-65402	
CVE-2026-65403	
CVE-2026-65404	
CVE-2026-65405	
CVE-2026-65406	
CVE-2026-65407	
CVE-2026-65408	
CVE-2026-65409	
CVE-2026-65410	
CVE-2026-65412	
CVE-2026-65413	
CVE-2026-65414	9.8 CRITICAL
CVE-2026-65415	8.1 HIGH
CVE-2026-84487	

CVE-2026-84489	5.5 MEDIUM
CVE-2026-84491	
CVE-2026-84492	4.7 MEDIUM
CVE-2026-84497	
CVE-2026-84505	7.8 HIGH
CVE-2026-84506	7.8 HIGH
CVE-2026-84507	
CVE-2026-84509	
CVE-2026-84510	
CVE-2026-84511	
CVE-2026-84512	
CVE-2026-84513	
CVE-2026-84514	
CVE-2026-84515	
CVE-2026-84516	
CVE-2026-84517	
CVE-2026-84518	4.3 MEDIUM
CVE-2026-84519	6.5 MEDIUM
CVE-2026-84520	
CVE-2026-84521	
CVE-2026-84522	
CVE-2026-84523	5.5 MEDIUM
CVE-2026-84524	

CVE-2026-84525	
CVE-2026-84526	
CVE-2026-84527	
CVE-2026-84530	
CVE-2026-84531	
CVE-2026-84532	
CVE-2026-84533	
CVE-2026-84534	
CVE-2026-84535	
CVE-2026-84536	
CVE-2026-84537	
CVE-2026-84538	6.5 MEDIUM
CVE-2026-84540	
CVE-2026-84541	
CVE-2026-84543	
CVE-2026-84544	
CVE-2026-84546	
CVE-2026-84548	
CVE-2026-84549	
CVE-2026-84550	
CVE-2026-84551	
CVE-2026-84552	
CVE-2026-84553	7.5 HIGH

CVE-2026-84554	5.9 MEDIUM
CVE-2026-84555	
CVE-2026-84556	
CVE-2026-84558	
CVE-2026-84559	
CVE-2026-84560	
CVE-2026-84561	
CVE-2026-84563	
CVE-2026-84564	
CVE-2026-84565	
CVE-2026-84566	
CVE-2026-84567	
CVE-2026-84568	7.8 HIGH
CVE-2026-84569	
CVE-2026-84570	
CVE-2026-84571	
CVE-2026-84572	
CVE-2026-84573	
CVE-2026-84574	
CVE-2026-84575	
CVE-2026-84576	
CVE-2026-84577	
CVE-2026-84578	

CVE-2026-84580	
CVE-2026-84581	
CVE-2026-84583	
CVE-2026-84584	
CVE-2026-84585	
CVE-2026-84586	5.5 MEDIUM
CVE-2026-84587	
CVE-2026-84588	6.5 MEDIUM
CVE-2026-84589	
CVE-2026-84596	6.5 MEDIUM
CVE-2026-84597	6.5 MEDIUM
CVE-2026-84600	
CVE-2026-84601	
CVE-2026-84602	
CVE-2026-84606	
CVE-2026-84607	7.8 HIGH
CVE-2026-84609	
CVE-2026-84611	7.3 HIGH
CVE-2026-84612	
CVE-2026-84616	
CVE-2026-84617	5.5 MEDIUM
CVE-2026-84618	
CVE-2026-84619	

CVE-2026-84620	
CVE-2026-84621	
CVE-2026-84622	
CVE-2026-84624	
CVE-2026-84625	
CVE-2026-84626	
CVE-2026-84628	
CVE-2026-84630	4.7 MEDIUM
CVE-2026-84631	7.8 HIGH
CVE-2026-84632	
CVE-2026-84635	
CVE-2026-86869	
CVE-2026-86870	
CVE-2026-86876	5.2 MEDIUM
CVE-2026-86881	
CVE-2026-86882	6.5 MEDIUM
CVE-2026-86884	
CVE-2026-86888	
CVE-2026-86889	4.8 MEDIUM
CVE-2026-86891	
CVE-2026-86894	
CVE-2026-86897	
CVE-2026-86898	

CVE-2026-86900	
CVE-2026-86901	
CVE-2026-86902	
CVE-2026-86903	5.5 MEDIUM
CVE-2026-86905	5.5 MEDIUM
CVE-2026-86909	
CVE-2026-86910	
CVE-2026-86911	
CVE-2026-86917	7.8 HIGH
CVE-2026-86924	

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-88	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-122	Heap-based Buffer Overflow
CWE-125	Out-of-bounds Read
CWE-190	Integer Overflow or Wraparound
CWE-280	Improper Handling of Insufficient Permissions or Privileges
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-451	User Interface (UI) Misrepresentation of Critical Information
CWE-642	External Control of Critical State Data
CWE-787	Out-of-bounds Write
CWE-862	Missing Authorization

Getroffen producten

Apple
macOS
macOS Golden Gate
macOS Sequoia
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.