



Advisory NCSC-2026-0455

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Apple MacOS

Publicatiedatum: 27-10-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Apple heeft meerdere kwetsbaarheden verholpen in macOS, met name in de versies Golden Gate 27.2, Sequoia 15.8.2, Tahoe 26.7.2 en Monterey 12.4.

Duiding

De kwetsbaarheden betroffen diverse beveiligingsaspecten binnen macOS, waaronder onvoldoende validatie van symbolische links (symlinks), onjuiste permissiecontroles, onvolledige autorisatiemechanismen, en fouten in geheugenbeheer zoals out-of-bounds reads en writes, use-after-free, buffer overflows, en race conditions. Deze fouten konden door lokale of remote aanvallers worden misbruikt om privileges te escaleren, sandbox-beperkingen te omzeilen, gevoelige gebruikersdata of kernelgeheugen te benaderen, of om denial-of-service condities te veroorzaken door onverwachte systeem- of applicatiecrashes.

Daarnaast werden problemen opgelost in Gatekeeper, de beveiligingscomponent die code-integriteit en app-verificatie afdwingt, waarbij bypasses werden voorkomen. Ook werden kwetsbaarheden in de verwerking van diverse bestandstypen zoals afbeeldingen, video's, audio, fonts, PDF's en ZIP-archieven aangepakt om geheugenbeschadiging en ongeautoriseerde code-uitvoering te voorkomen.

De fixes omvatten verbeterde validatie van invoer, strengere toegangscontroles, verbeterde geheugenbeheer en state management, en het versterken van sandbox- en privacymechanismen. De updates zijn ook doorgevoerd in andere Apple-platforms zoals tvOS, visionOS en watchOS, waarbij consistentie in beveiligingsverbeteringen werd nagestreefd.

Oplossingen

Apple heeft updates uitgebracht voor macOS Golden Gate 27.2, Sequoia 15.8.2, Tahoe 26.7.2, Monterey 12.4 en andere versies om de beschreven kwetsbaarheden te verhelpen. Deze updates bevatten verbeterde validatie- en beveiligingsmechanismen die de integriteit, stabiliteit en privacy van het systeem versterken. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://support.apple.com/en-us/149521>
- <https://support.apple.com/en-us/149522>
- <https://support.apple.com/en-us/149523>

Kwetsbaarheden

CVE	CVSS Score
CVE-2022-26704	
CVE-2026-20648	5.5 MEDIUM
CVE-2026-20649	7.5 HIGH
CVE-2026-28864	3.3 LOW
CVE-2026-28991	7.5 HIGH
CVE-2026-43736	
CVE-2026-64750	
CVE-2026-64767	9.8 CRITICAL
CVE-2026-64789	
CVE-2026-65327	8.4 HIGH
CVE-2026-65350	
CVE-2026-65363	
CVE-2026-65368	
CVE-2026-65373	
CVE-2026-65384	
CVE-2026-65392	
CVE-2026-65397	
CVE-2026-84494	
CVE-2026-84495	
CVE-2026-84496	6.5 MEDIUM
CVE-2026-84498	
CVE-2026-84528	

CVE	CVSS Score
CVE-2026-84539	
CVE-2026-84542	
CVE-2026-84545	
CVE-2026-84590	
CVE-2026-84595	
CVE-2026-84604	
CVE-2026-84610	
CVE-2026-84627	
CVE-2026-86896	
CVE-2026-86916	7.8 HIGH
CVE-2026-86920	
CVE-2026-86923	
CVE-2026-86925	
CVE-2026-86929	8.8 HIGH
CVE-2026-86931	
CVE-2026-86936	
CVE-2026-86937	
CVE-2026-86939	
CVE-2026-86941	
CVE-2026-86942	
CVE-2026-86943	
CVE-2026-86945	
CVE-2026-86946	
CVE-2026-86954	
CVE-2026-86958	
CVE-2026-86964	
CVE-2026-86966	
CVE-2026-86968	
CVE-2026-86969	
CVE-2026-86970	
CVE-2026-86971	6.5 MEDIUM
CVE-2026-86972	

CVE	CVSS Score
CVE-2026-86973	
CVE-2026-86974	
CVE-2026-86978	
CVE-2026-86984	
CVE-2026-86985	
CVE-2026-86986	
CVE-2026-86988	
CVE-2026-86990	
CVE-2026-86991	
CVE-2026-86992	
CVE-2026-112410	
CVE-2026-112413	
CVE-2026-112414	
CVE-2026-112415	6.5 MEDIUM
CVE-2026-112416	
CVE-2026-112421	
CVE-2026-112423	
CVE-2026-112424	
CVE-2026-112425	
CVE-2026-112427	8.1 HIGH
CVE-2026-112428	
CVE-2026-112429	
CVE-2026-112430	
CVE-2026-112432	
CVE-2026-112434	
CVE-2026-112437	
CVE-2026-112438	8.8 HIGH
CVE-2026-112441	
CVE-2026-112442	
CVE-2026-112443	
CVE-2026-112444	
CVE-2026-112446	

CVE	CVSS Score
CVE-2026-112447	
CVE-2026-112449	
CVE-2026-112451	
CVE-2026-112453	
CVE-2026-112454	
CVE-2026-112455	
CVE-2026-112456	
CVE-2026-112457	7.1 HIGH
CVE-2026-112459	
CVE-2026-112461	
CVE-2026-112462	
CVE-2026-112464	
CVE-2026-112466	
CVE-2026-112467	
CVE-2026-112468	
CVE-2026-112469	
CVE-2026-112470	
CVE-2026-112471	4.3 MEDIUM
CVE-2026-112473	
CVE-2026-112474	
CVE-2026-112475	
CVE-2026-112476	
CVE-2026-112477	
CVE-2026-112478	
CVE-2026-112479	
CVE-2026-112480	
CVE-2026-112481	
CVE-2026-112482	
CVE-2026-112483	
CVE-2026-112484	7.8 HIGH
CVE-2026-112485	
CVE-2026-112486	

CVE	CVSS Score
CVE-2026-112487	
CVE-2026-112488	
CVE-2026-112491	
CVE-2026-112492	
CVE-2026-112493	
CVE-2026-112494	
CVE-2026-112495	
CVE-2026-112497	
CVE-2026-112498	
CVE-2026-112500	
CVE-2026-112501	
CVE-2026-112502	
CVE-2026-112504	
CVE-2026-112505	
CVE-2026-112506	
CVE-2026-112508	
CVE-2026-112510	
CVE-2026-112511	
CVE-2026-112512	
CVE-2026-112513	
CVE-2026-112514	
CVE-2026-112515	
CVE-2026-112516	
CVE-2026-112517	
CVE-2026-112518	
CVE-2026-112519	
CVE-2026-112521	
CVE-2026-112522	
CVE-2026-112523	
CVE-2026-112524	
CVE-2026-112525	
CVE-2026-112526	

CVE	CVSS Score
CVE-2026-112529	
CVE-2026-112530	
CVE-2026-112531	
CVE-2026-112532	
CVE-2026-112533	
CVE-2026-112534	
CVE-2026-112535	
CVE-2026-112536	
CVE-2026-112537	
CVE-2026-112539	
CVE-2026-112540	
CVE-2026-112541	
CVE-2026-112542	
CVE-2026-112543	
CVE-2026-112544	6.5 MEDIUM
CVE-2026-112545	
CVE-2026-112546	
CVE-2026-112548	
CVE-2026-112550	
CVE-2026-112551	
CVE-2026-112552	
CVE-2026-112553	
CVE-2026-112554	
CVE-2026-112555	
CVE-2026-112556	4.8 MEDIUM
CVE-2026-112557	
CVE-2026-112558	
CVE-2026-112559	
CVE-2026-112560	
CVE-2026-112561	
CVE-2026-112562	
CVE-2026-112563	

CVE	CVSS Score
CVE-2026-112565	
CVE-2026-112566	
CVE-2026-112567	
CVE-2026-112568	
CVE-2026-112569	
CVE-2026-112570	
CVE-2026-112571	
CVE-2026-112575	
CVE-2026-112576	
CVE-2026-112577	
CVE-2026-112593	
CVE-2026-112595	
CVE-2026-112596	
CVE-2026-112599	
CVE-2026-112601	
CVE-2026-112604	
CVE-2026-112606	
CVE-2026-112607	
CVE-2026-112610	
CVE-2026-112611	
CVE-2026-112614	6.5 MEDIUM
CVE-2026-112615	
CVE-2026-112616	
CVE-2026-112617	
CVE-2026-112619	
CVE-2026-112620	
CVE-2026-112621	
CVE-2026-112622	
CVE-2026-112623	8.8 HIGH
CVE-2026-112624	
CVE-2026-112625	
CVE-2026-112626	8.8 HIGH

CVE	CVSS Score
CVE-2026-112627	
CVE-2026-112628	
CVE-2026-112629	6.5 MEDIUM
CVE-2026-112630	
CVE-2026-112632	
CVE-2026-112633	6.5 MEDIUM
CVE-2026-112634	6.5 MEDIUM
CVE-2026-112637	8.8 HIGH
CVE-2026-112638	
CVE-2026-112639	
CVE-2026-112640	
CVE-2026-112642	
CVE-2026-112647	
CVE-2026-112651	8.8 HIGH
CVE-2026-112652	
CVE-2026-112653	
CVE-2026-112654	
CVE-2026-112655	8.8 HIGH
CVE-2026-112656	
CVE-2026-112658	
CVE-2026-112659	8.8 HIGH
CVE-2026-112660	
CVE-2026-112665	
CVE-2026-112666	
CVE-2026-112668	
CVE-2026-112669	
CVE-2026-112670	
CVE-2026-112671	
CVE-2026-112672	
CVE-2026-112673	
CVE-2026-112675	
CVE-2026-112676	

CVE	CVSS Score
CVE-2026-112677	
CVE-2026-112678	
CVE-2026-112679	
CVE-2026-112680	
CVE-2026-112682	
CVE-2026-112683	
CVE-2026-112684	
CVE-2026-112685	
CVE-2026-112686	
CVE-2026-112688	8.8 HIGH
CVE-2026-112689	
CVE-2026-112690	
CVE-2026-112693	
CVE-2026-112695	
CVE-2026-112696	
CVE-2026-112697	
CVE-2026-112698	
CVE-2026-112699	
CVE-2026-112704	
CVE-2026-112705	
CVE-2026-112708	5.3 MEDIUM
CVE-2026-113896	
CVE-2026-113897	
CVE-2026-113898	
CVE-2026-113899	
CVE-2026-113900	
CVE-2026-113901	
CVE-2026-113903	
CVE-2026-113904	
CVE-2026-113907	6.1 MEDIUM
CVE-2026-113909	
CVE-2026-113910	

CVE	CVSS Score
CVE-2026-113912	
CVE-2026-113913	6.5 MEDIUM
CVE-2026-113915	
CVE-2026-113934	
CVE-2026-113935	
CVE-2026-113936	
CVE-2026-113937	
CVE-2026-113938	
CVE-2026-113939	6.5 MEDIUM
CVE-2026-113940	
CVE-2026-113941	
CVE-2026-113942	
CVE-2026-113943	6.5 MEDIUM
CVE-2026-113944	
CVE-2026-113945	
CVE-2026-113946	
CVE-2026-113947	8.8 HIGH
CVE-2026-113948	
CVE-2026-113949	
CVE-2026-113950	
CVE-2026-113952	

CWE's

CWE	Beschrijving
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-125	Out-of-bounds Read
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

CWE	Beschrijving
CWE-377	Insecure Temporary File
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-863	Incorrect Authorization

Getroffen producten

Apple

macOS

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 or 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.