Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0267

Kwetsbaarheden verholpen in Apple MacOS

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 28-07-2026

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 in de versies Sequoia 15.7.8, Sonoma 14.8.8 en Tahoe 26.x.

Duiding

De kwetsbaarheden betreffen diverse beveiligingsproblemen in macOS, waaronder onvoldoende sandbox restricties waardoor applicaties mogelijk ongeautoriseerd toegang kunnen krijgen tot gevoelige gebruikersdata. Er zijn problemen opgelost met betrekking tot onjuiste geheugenafhandeling, zoals use-after-free, buffer overflows, out-of-bounds reads en writes, integer overflows, race conditions en type confusion. Deze kunnen leiden tot onverwachte systeem- of applicatie-terminaties, privilege escalatie, ongeautoriseerde toegang tot kernel geheugen, en in sommige gevallen remote code execution.

Daarnaast zijn er fixes voor bypasses van Gatekeeper beveiliging via gemanipuleerde ZIP-archieven, verbeterde validatie van bestands- en padverwerking, en versterkte autorisatie- en toestemmingscontroles. Ook zijn er verbeteringen doorgevoerd in de netwerkbeveiliging, zoals het voorkomen van het onderscheppen van netwerkverbindingen en het beperken van applicatie permissies.

De updates richten zich op het versterken van geheugenbeheer, inputvalidatie, state management en sandbox isolatie om ongeautoriseerde toegang en systeeminstabiliteit te voorkomen. De kwetsbaarheden zijn opgelost in de genoemde macOS versies en sommige fixes zijn ook doorgevoerd in gerelateerde Apple besturingssystemen zoals iOS, iPadOS, tvOS, visionOS en watchOS.

Oplossingen

Apple heeft updates uitgebracht voor macOS Sequoia 15.7.8, Sonoma 14.8.8 en Tahoe 26.x die deze kwetsbaarheden verhelpen door verbeterde sandbox restricties, geheugenbeheer, inputvalidatie, autorisatiecontroles en andere beveiligingsmechanismen te implementeren. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://support.apple.com/en-us/128067
- https://support.apple.com/en-us/128071
- https://support.apple.com/en-us/128072

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-43325	4.8 MEDIUM
CVE-2026-3783	6.3 MEDIUM
CVE-2026-3784	6.3 MEDIUM
CVE-2026-4424	6.9 MEDIUM
CVE-2026-20672	
CVE-2026-23918	6.9 MEDIUM
CVE-2026-28849	
CVE-2026-28896	
CVE-2026-28900	
CVE-2026-28911	
CVE-2026-28912	
CVE-2026-28914	5.5 MEDIUM
CVE-2026-28926	
CVE-2026-28928	
CVE-2026-28931	
CVE-2026-28932	
CVE-2026-28936	7.5 HIGH
CVE-2026-28945	
CVE-2026-28961	4.6 MEDIUM
CVE-2026-28973	
CVE-2026-28981	

CVE-2026-28982	
CVE-2026-28983	7.5 HIGH
CVE-2026-39868	9.1 CRITICAL
CVE-2026-39873	
CVE-2026-39874	7.8 HIGH
CVE-2026-39875	7.8 HIGH
CVE-2026-39877	
CVE-2026-43653	6.2 MEDIUM
CVE-2026-43661	7.5 HIGH
CVE-2026-43665	
CVE-2026-43672	
CVE-2026-43673	
CVE-2026-43681	
CVE-2026-43682	
CVE-2026-43693	7.0 HIGH
CVE-2026-43694	
CVE-2026-43698	7.8 HIGH
CVE-2026-43703	6.5 MEDIUM
CVE-2026-43706	6.5 MEDIUM
CVE-2026-43710	
CVE-2026-43711	
CVE-2026-43714	
CVE-2026-43722	4.8 MEDIUM

CVE-2026-43723	7.8 HIGH
CVE-2026-43724	4.8 MEDIUM
CVE-2026-43728	
CVE-2026-43729	
CVE-2026-43730	
CVE-2026-43733	
CVE-2026-43738	
CVE-2026-43739	
CVE-2026-43740	5.3 MEDIUM
CVE-2026-43744	
CVE-2026-43747	
CVE-2026-43748	
CVE-2026-43749	7.8 HIGH
CVE-2026-43750	
CVE-2026-43753	
CVE-2026-43754	
CVE-2026-43755	7.0 HIGH
CVE-2026-43756	
CVE-2026-43757	
CVE-2026-43758	
CVE-2026-43759	
CVE-2026-43760	
CVE-2026-43763	

- CVE-2026-43764
- CVE-2026-43765
- CVE-2026-43766
- CVE-2026-43767
- CVE-2026-43768
- CVE-2026-43769
- CVE-2026-43770
- CVE-2026-43771
- CVE-2026-43772
- CVE-2026-43773
- CVE-2026-43774
- CVE-2026-43775
- CVE-2026-43776 **7.8 HIGH**
- CVE-2026-43777
- CVE-2026-43778
- CVE-2026-43779
- CVE-2026-43780
- CVE-2026-43781
- CVE-2026-43782
- CVE-2026-43792
- CVE-2026-43793
- CVE-2026-43796
- CVE-2026-43797

- CVE-2026-43799
- CVE-2026-43800
- CVE-2026-43801
- CVE-2026-43802
- CVE-2026-43803
- CVE-2026-43804
- CVE-2026-43805
- CVE-2026-43806
- CVE-2026-43807
- CVE-2026-43809
- CVE-2026-43810
- CVE-2026-43812
- CVE-2026-43813
- CVE-2026-43814
- CVE-2026-43816
- CVE-2026-43817
- CVE-2026-43818
- CVE-2026-43819
- CVE-2026-43821
- CVE-2026-43822
- CVE-2026-64691
- CVE-2026-64692
- CVE-2026-64693

- CVE-2026-64694
- CVE-2026-64695
- CVE-2026-64696
- CVE-2026-64697
- CVE-2026-64698
- CVE-2026-64699
- CVE-2026-64700
- CVE-2026-64702
- CVE-2026-64703
- CVE-2026-64704
- CVE-2026-64707
- CVE-2026-64708
- CVE-2026-64709
- CVE-2026-64710
- CVE-2026-64711
- CVE-2026-64713
- CVE-2026-64716
- CVE-2026-64718
- CVE-2026-64719
- CVE-2026-64720
- CVE-2026-64721
- CVE-2026-64722
- CVE-2026-64723

- CVE-2026-64724
- CVE-2026-64725
- CVE-2026-64726
- CVE-2026-64727
- CVE-2026-64728
- CVE-2026-64729
- CVE-2026-64730
- CVE-2026-64731
- CVE-2026-64733
- CVE-2026-64734
- CVE-2026-64735
- CVE-2026-64737
- CVE-2026-64738
- CVE-2026-64739
- CVE-2026-64740
- CVE-2026-64743
- CVE-2026-64744
- CVE-2026-64745
- CVE-2026-64746
- CVE-2026-64747
- CVE-2026-64749
- CVE-2026-64751
- CVE-2026-64754

CVE-2026-64757	
CVE-2026-64758	9.4 CRITICAL
CVE-2026-64762	2.4 LOW
CVE-2026-64763	10.0 CRITICAL
CVE-2026-64764	9.4 CRITICAL
CVE-2026-64765	9.4 CRITICAL
CVE-2026-64766	9.4 CRITICAL
CVE-2026-64767	10.0 CRITICAL
CVE-2026-64768	5.3 MEDIUM
CVE-2026-64769	9.4 CRITICAL
CVE-2026-64770	9.4 CRITICAL
CVE-2026-64771	9.4 CRITICAL
CVE-2026-64772	9.4 CRITICAL
CVE-2026-64774	9.4 CRITICAL
CVE-2026-64775	6.8 MEDIUM
CVE-2026-64776	5.1 MEDIUM
CVE-2026-64783	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-88	

Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	
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-121	Stack-based Buffer Overflow
CWE-125	Out-of-bounds Read
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-201	Insertion of Sensitive Information Into Sent Data
CWE-276	Incorrect Default Permissions
CWE-284	Improper Access Control
CWE-305	Authentication Bypass by Primary Weakness
CWE-358	Improperly Implemented Security Check for Standard
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-400	Uncontrolled Resource Consumption
CWE-404	Improper Resource Shutdown or Release
CWE-415	Double Free
CWE-416	Use After Free
CWE-522	Insufficiently Protected Credentials
CWE-693	Protection Mechanism Failure
CWE-787	Out-of-bounds Write
CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')
CWE-1341	Multiple Releases of Same Resource or Handle

Getroffen producten

Apple
Mac OS
macOS Sequoia
macOS Sonoma
macOS Tahoe

Disclaimer