Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0151

Kwetsbaarheden verholpen in Apple macOS

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 13-05-2025

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 (Specifiek voor Ventura 13.7.6, Sequoia 15.5 en Sonoma 14.7.6).

Duiding

De kwetsbaarheden omvatten verschillende problemen, zoals geheugenbeschadiging door het verwerken van kwaadwillig gemaakte webinhoud, ongeautoriseerde toegang tot gevoelige gebruikersdata, en onverwachte systeemterminaties. Deze kwetsbaarheden kunnen worden misbruikt door kwaadwillenden om zich verhoogde rechten toe te kennen en zo toegang te krijgen tot gevoelige informatie of om de stabiliteit van het systeem in gevaar te brengen.

Oplossingen

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

Referenties

- https://support.apple.com/en-us/122718
- https://support.apple.com/en-us/122717
- https://support.apple.com/en-us/122716

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-8176	5.1 MEDIUM
CVE-2025-24142	
CVE-2025-24144	
CVE-2025-24155	
CVE-2025-24213	8.8 HIGH
CVE-2025-24222	

CVE-2025-24223	
CVE-2025-24258	
CVE-2025-24274	
CVE-2025-26465	6.3 MEDIUM
CVE-2025-26466	6.9 MEDIUM
CVE-2025-30440	
CVE-2025-30442	
CVE-2025-30443	5.5 MEDIUM
CVE-2025-30448	
CVE-2025-30453	
CVE-2025-31196	
CVE-2025-31204	
CVE-2025-31205	
CVE-2025-31206	
CVE-2025-31208	
CVE-2025-31209	
CVE-2025-31212	
CVE-2025-31213	
CVE-2025-31215	
CVE-2025-31217	
CVE-2025-31218	4.8 MEDIUM
CVE-2025-31219	
CVE-2025-31220	4.8 MEDIUM

CVE-2025-31221	
CVE-2025-31222	
CVE-2025-31223	
CVE-2025-31224	4.8 MEDIUM
CVE-2025-31226	
CVE-2025-31232	4.8 MEDIUM
CVE-2025-31233	5.3 MEDIUM
CVE-2025-31234	
CVE-2025-31235	6.8 MEDIUM
CVE-2025-31236	4.8 MEDIUM
CVE-2025-31237	
CVE-2025-31238	
CVE-2025-31239	5.3 MEDIUM
CVE-2025-31240	
CVE-2025-31241	5.3 MEDIUM
CVE-2025-31242	4.8 MEDIUM
CVE-2025-31244	4.8 MEDIUM
CVE-2025-31245	6.8 MEDIUM
CVE-2025-31246	9.2 CRITICAL
CVE-2025-31247	
CVE-2025-31249	4.8 MEDIUM
CVE-2025-31250	4.8 MEDIUM
CVE-2025-31251	5.3 MEDIUM

CVE-2025-31256	**4.8 MEDIUM**
CVE-2025-31257	
CVE-2025-31258	**4.8 MEDIUM**
CVE-2025-31259	**4.8 MEDIUM**
CVE-2025-31260	**4.8 MEDIUM**

CWE's

CWE	Beschrijving
CWE-390	Detection of Error Condition Without Action
CWE-310	CWE-310
CWE-415	Double Free
CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')
CWE-265	CWE-265
CWE-404	Improper Resource Shutdown or Release
CWE-275	CWE-275
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
CWE-416	Use After Free
CWE-400	Uncontrolled Resource Consumption
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-674	Uncontrolled Recursion
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-121	Stack-based Buffer Overflow

Getroffen producten

Apple
macOS

Disclaimer