Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0381

Kwetsbaarheden verholpen in Apple MacOS

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 26-09-2024

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

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot de volgende categorieën schade:

- Denial-of-Service (DoS)
- Manipulatie van gegevens
- Omzeilen van beveiligingsmaatregel
- Toegang tot gevoelige gegevens
- Toegang tot systeemgegevens

Voor succesvol misbruik moet de kwaadwillende lokale toegang hebben, het slachtoffer misleiden een malafide app te downloaden en installeren, of een malafide bestand te openen of link te volgen.

Oplossingen

Apple heeft updates uitgebracht om de kwetsbaarheden te verhelpen in MacOS 13.7, 14.7 en 15. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://support.apple.com/en-us/121247
- https://support.apple.com/en-us/121234
- https://support.apple.com/en-us/121238

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-44154	5.5 MEDIUM
CVE-2024-44158	5.5 MEDIUM
CVE-2024-44160	7.8 HIGH
CVE-2024-44161	

CVE-2024-44163	
CVE-2024-44164	
CVE-2024-44165	
CVE-2024-44166	
CVE-2024-44167	8.1 HIGH
CVE-2024-44168	
CVE-2024-44169	8.1 HIGH
CVE-2024-44170	
CVE-2024-44176	5.5 MEDIUM
CVE-2024-44177	5.5 MEDIUM
CVE-2024-44178	
CVE-2024-44181	5.5 MEDIUM
CVE-2024-44182	5.5 MEDIUM
CVE-2024-44183	
CVE-2024-44184	5.5 MEDIUM
CVE-2024-44186	5.5 MEDIUM
CVE-2024-44187	6.5 MEDIUM
CVE-2024-44188	5.5 MEDIUM
CVE-2024-44189	7.5 HIGH
CVE-2024-44190	5.5 MEDIUM
CVE-2024-44191	5.5 MEDIUM
CVE-2024-44198	5.5 MEDIUM
CVE-2023-4504	7.8 HIGH

CVE-2023-5841	9.1 CRITICAL
CVE-2024-23237	5.5 MEDIUM
CVE-2024-27795	7.5 HIGH
CVE-2024-27858	5.5 MEDIUM
CVE-2024-27860	5.5 MEDIUM
CVE-2024-27861	7.5 HIGH
CVE-2024-27869	7.5 HIGH
CVE-2024-27875	5.5 MEDIUM
CVE-2024-27876	8.1 HIGH
CVE-2024-27880	5.5 MEDIUM
CVE-2024-27886	
CVE-2024-39894	7.5 HIGH
CVE-2024-40770	7.5 HIGH
CVE-2024-40791	3.3 LOW
CVE-2024-40797	6.1 MEDIUM
CVE-2024-40801	5.5 MEDIUM
CVE-2024-40814	
CVE-2024-40825	6.0 MEDIUM
CVE-2024-40826	6.1 MEDIUM
CVE-2024-40831	5.5 MEDIUM
CVE-2024-40837	5.5 MEDIUM
CVE-2024-40838	3.3 LOW
CVE-2024-40841	7.8 HIGH

CVE-2024-40842	5.5 MEDIUM
CVE-2024-40843	5.5 MEDIUM
CVE-2024-40844	5.5 MEDIUM
CVE-2024-40845	5.5 MEDIUM
CVE-2024-40846	5.5 MEDIUM
CVE-2024-40847	5.5 MEDIUM
CVE-2024-40848	7.5 HIGH
CVE-2024-40850	5.5 MEDIUM
CVE-2024-40856	7.5 HIGH
CVE-2024-40857	7.1 HIGH
CVE-2024-40859	5.5 MEDIUM
CVE-2024-40860	
CVE-2024-40861	7.8 HIGH
CVE-2024-40866	6.5 MEDIUM
CVE-2024-41957	5.3 MEDIUM
CVE-2024-44125	5.5 MEDIUM
CVE-2024-44128	
CVE-2024-44129	5.5 MEDIUM
CVE-2024-44130	4.4 MEDIUM
CVE-2024-44131	5.5 MEDIUM
CVE-2024-44132	8.4 HIGH
CVE-2024-44133	5.5 MEDIUM
CVE-2024-44134	5.5 MEDIUM

CVE-2024-44135	5.5 MEDIUM
CVE-2024-44146	10.0 CRITICAL
CVE-2024-44148	10.0 CRITICAL
CVE-2024-44149	7.5 HIGH
CVE-2024-44151	
CVE-2024-44152	7.5 HIGH
CVE-2024-44153	5.5 MEDIUM

CWE's

CWE	Beschrijving
CWE-208	Observable Timing Discrepancy
CWE-942	Permissive Cross-domain Policy with Untrusted Domains
CWE-415	Double Free
CWE-265	CWE-265
CWE-203	Observable Discrepancy
CWE-190	Integer Overflow or Wraparound
CWE-61	UNIX Symbolic Link (Symlink) Following
CWE-285	Improper Authorization
CWE-404	Improper Resource Shutdown or Release
CWE-275	CWE-275
CWE-284	Improper Access Control
CWE-377	Insecure Temporary File
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor

CWE-122	Heap-based Buffer Overflow
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

apple
macos_sequoia__15
macos_sonoma__14.7
macos_ventura__13.7

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.