



NCSC-2024-0217

Kwetsbaarheden verholpen in Apple MacOS

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 15-05-2024

Revisie: 1.0.1

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

Update Revisie 1

Initiele versie

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
- (Remote) code execution (Gebruikersrechten)
- (Remote) code execution (Administrator/Root rechten)
- Toegang tot gevoelige gegevens
- Toegang tot systeemgegevens
- Verhoogde gebruikersrechten

Van de kwetsbaarheid met kenmerk CVE-2024-23296 geeft Apple aan informatie te hebben dat deze beperkt en gericht is misbruikt. De kwetsbaarheid bevindt zich in de module RTKit en stelt een lokale kwaadwillende, met rechten om kernelgeheugen te lezen en te schrijven, de geheugenbescherming van de kernel te omzeilen en zo toegang te krijgen tot delen van het werkgeheugen waartoe de kwaadwillende aanvankelijk niet is geautoriseerd.

Oplossingen

Apple heeft updates uitgebracht om de kwetsbaarheden te verhelpen in MacOS 14.5, 13.6.7 en 12.7.5

Referenties

- <https://support.apple.com/en-us/HT214105>
- <https://support.apple.com/en-us/HT214107>
- <https://support.apple.com/en-us/HT214106>

Kwetsbaarheden

CVE	CVSS Score
> CVE-2023-42893	5.5 MEDIUM
> CVE-2024-23236	
> CVE-2024-27796	
> CVE-2024-27798	
> CVE-2024-27804	
> CVE-2024-27810	
> CVE-2024-27813	
> CVE-2024-27816	
> CVE-2024-27818	
> CVE-2024-27821	
> CVE-2024-27822	
> CVE-2024-27824	
> CVE-2024-27825	
> CVE-2024-27827	
> CVE-2024-27829	
> CVE-2024-27834	
> CVE-2024-27837	
> CVE-2024-27841	
> CVE-2024-27842	
> CVE-2024-27843	
> CVE-2024-27847	

CWE's

CWE	Beschrijving
> CWE-840	CWE-840
> CWE-265	CWE-265
> CWE-371	CWE-371
> CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
> CWE-284	Improper Access Control
> CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
> CWE-285	Improper Authorization
> CWE-757	Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade')

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 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.