



# NCSC-2024-0320

## Kwetsbaarheden verholpen in Apple MacOS

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 30-07-2024

**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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto:info@ncsc.nl)

## Feiten

Apple heeft kwetsbaarheden verholpen in MacOS.

## Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om een beveiligingsmaatregel te omzeilen, zichzelf verhoogde rechten toe te kennen, toegang te krijgen tot gevoelige gegevens, willekeurige code uit te voeren, mogelijk met kernel-rechten of een Denial-of-Service te veroorzaken.

Voor succesvol misbruik moet de kwaadwillende het slachtoffer misleiden een malafide app te installeren en draaien, of een malafide link te volgen. Voor het uitvoeren van willekeurige code met kernel-rechten moet de kwaadwillende reeds beschikken over verhoogde rechten op het kwetsbare systeem.

## Oplossingen

Apple heeft updates uitgebracht om de kwetsbaarheden te verhelpen in MacOS 12.7.6, 13.6.8 en 14.6. Zie bijgevoegde referenties voor meer informatie.

## Referenties

- <https://support.apple.com/en-us/HT214118>
- <https://support.apple.com/en-us/HT214119>
- <https://support.apple.com/en-us/HT214120>

## Kwetsbaarheden

CVE	CVSS Score
➤ <a href="#">CVE-2023-6277</a>	
➤ <a href="#">CVE-2023-27952</a>	<b>4.7 MEDIUM</b>
➤ <a href="#">CVE-2023-38709</a>	
➤ <a href="#">CVE-2023-52356</a>	
➤ <a href="#">CVE-2024-2004</a>	
➤ <a href="#">CVE-2024-2379</a>	

> CVE-2024-2398	
> CVE-2024-2466	
> CVE-2024-4558	
> CVE-2024-6387	
> CVE-2024-23261	
> CVE-2024-23296	7.8 HIGH
> CVE-2024-24795	
> CVE-2024-27316	
> CVE-2024-27826	
> CVE-2024-27862	
> CVE-2024-27863	
> CVE-2024-27871	
> CVE-2024-27872	
> CVE-2024-27873	
> CVE-2024-27877	
> CVE-2024-27878	
> CVE-2024-27881	
> CVE-2024-27882	
> CVE-2024-27883	
> CVE-2024-40774	
> CVE-2024-40775	
> CVE-2024-40776	
> CVE-2024-40777	

<a href="#">&gt; CVE-2024-40778</a>
<a href="#">&gt; CVE-2024-40779</a>
<a href="#">&gt; CVE-2024-40780</a>
<a href="#">&gt; CVE-2024-40781</a>
<a href="#">&gt; CVE-2024-40782</a>
<a href="#">&gt; CVE-2024-40783</a>
<a href="#">&gt; CVE-2024-40784</a>
<a href="#">&gt; CVE-2024-40785</a>
<a href="#">&gt; CVE-2024-40786</a>
<a href="#">&gt; CVE-2024-40787</a>
<a href="#">&gt; CVE-2024-40788</a>
<a href="#">&gt; CVE-2024-40789</a>
<a href="#">&gt; CVE-2024-40793</a>
<a href="#">&gt; CVE-2024-40794</a>
<a href="#">&gt; CVE-2024-40795</a>
<a href="#">&gt; CVE-2024-40796</a>
<a href="#">&gt; CVE-2024-40798</a>
<a href="#">&gt; CVE-2024-40799</a>
<a href="#">&gt; CVE-2024-40800</a>
<a href="#">&gt; CVE-2024-40802</a>
<a href="#">&gt; CVE-2024-40803</a>
<a href="#">&gt; CVE-2024-40804</a>
<a href="#">&gt; CVE-2024-40805</a>

> [CVE-2024-40806](#)

> [CVE-2024-40807](#)

> [CVE-2024-40809](#)

> [CVE-2024-40811](#)

> [CVE-2024-40812](#)

> [CVE-2024-40814](#)

> [CVE-2024-40815](#)

> [CVE-2024-40816](#)

> [CVE-2024-40817](#)

> [CVE-2024-40818](#)

> [CVE-2024-40821](#)

> [CVE-2024-40822](#)

> [CVE-2024-40823](#)

> [CVE-2024-40824](#)

> [CVE-2024-40827](#)

> [CVE-2024-40828](#)

> [CVE-2024-40829](#)

> [CVE-2024-40832](#)

> [CVE-2024-40833](#)

> [CVE-2024-40834](#)

> [CVE-2024-40835](#)

> [CVE-2024-40836](#)

## CWE's

CWE	Beschrijving
> CWE-1021	Improper Restriction of Rendered UI Layers or Frames
> CWE-113	Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting')
> CWE-115	Misinterpretation of Input
> 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-122	Heap-based Buffer Overflow
> CWE-20	Improper Input Validation
> CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
> CWE-284	Improper Access Control
> CWE-295	Improper Certificate Validation
> CWE-297	Improper Validation of Certificate with Host Mismatch
> CWE-319	Cleartext Transmission of Sensitive Information
> CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
> CWE-364	Signal Handler Race Condition
> CWE-400	Uncontrolled Resource Consumption
> CWE-401	Missing Release of Memory after Effective Lifetime
> CWE-404	Improper Resource Shutdown or Release
> CWE-770	Allocation of Resources Without Limits or Throttling
> CWE-772	Missing Release of Resource after Effective Lifetime
> CWE-787	Out-of-bounds Write

## 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.