



NCSC-2025-0266

Kwetsbaarheid verholpen in Apple MacOS, iOS en iPadOS

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 25-08-2025

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

Informatie over proof-of-conceptcode toegevoegd.

Feiten

Apple heeft een kwetsbaarheid verholpen in verschillende Apple besturingssystemen.

Duiding

De kwetsbaarheid bevindt zich in de wijze waarop de systemen omgaan met het verwerken van kwaadaardige afbeeldingsbestanden, wat kan leiden tot geheugen corruptie. Dit probleem is aangepakt door verbeterde controles op geheugenlimieten.

Apple geeft aan informatie te hebben dat deze kwetsbaarheid beperkt en zeer gericht actief is misbruikt. Op het internet is proof-of-conceptcode (PoC-code) verschenen waarmee de kwetsbaarheid kan worden misbruikt. Het bestaan van een PoC vergroot de kans op misbruik. Het NCSC heeft de werking van het PoC echter niet geverifieerd.

Oplossingen

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

Referenties

- <https://support.apple.com/en-us/124925>
- <https://support.apple.com/en-us/124926>
- <https://support.apple.com/en-us/124927>
- <https://support.apple.com/en-us/124928>
- <https://support.apple.com/en-us/124929>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-43300	5.3 MEDIUM

CWE's

CWE	Beschrijving
> CWE-787	Out-of-bounds Write

Getroffen producten

Apple
iOS
macOS Sequoia
macOS Sonoma
macOS Ventura
iOS and iPadOS

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.