Nationaal Cyber Security Centrum
*Ministerie van Justitie en Veiligheid*

# NCSC-2026-0102

## Kwetsbaarheden verholpen in Apple macOS

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 25-03-2026

**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 meerdere kwetsbaarheden verholpen in macOS (Specifiek voor Sequoia 15.7.5, Sonoma 14.8.5, en Tahoe 26.4).

## Duiding

De kwetsbaarheden omvatten verschillende problemen zoals onvoldoende validatie van invoer, onjuiste afhandeling van geheugen, en problemen met machtigingen die konden leiden tot ongeautoriseerde toegang tot gevoelige gebruikersdata. Aanvallers kunnen deze kwetsbaarheden misbruiken om toegang te krijgen tot beschermde systeembestanden, gegevens te wijzigen, of zelfs de stabiliteit van het systeem in gevaar te brengen. De kwetsbaarheden zijn opgelost door verbeterde validatie- en beveiligingsmechanismen in de betrokken macOS-versies.

## Oplossingen

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

## Referenties

- https://support.apple.com/en-us/126794
- https://support.apple.com/en-us/126795
- https://support.apple.com/en-us/126796

## Kwetsbaarheden

| CVE | CVSS Score |
| --- | --- |
| CVE-2025-14524 | 5.3 MEDIUM |
| CVE-2025-55753 | 6.9 MEDIUM |
| CVE-2025-58098 | 6.3 MEDIUM |
| CVE-2025-59775 | 2.3 LOW |
| CVE-2025-64505 | 5.3 MEDIUM |
| CVE-2025-65082 | 5.1 MEDIUM |

| | |
|---|---|
| CVE-2025-66200 | 2.3 LOW |
| CVE-2026-20607 | |
| CVE-2026-20631 | |
| CVE-2026-20632 | |
| CVE-2026-20633 | |
| CVE-2026-20637 | |
| CVE-2026-20639 | |
| CVE-2026-20643 | 5.3 MEDIUM |
| CVE-2026-20651 | |
| CVE-2026-20657 | |
| CVE-2026-20660 | 7.5 HIGH |
| CVE-2026-20664 | |
| CVE-2026-20665 | |
| CVE-2026-20668 | |
| CVE-2026-20684 | |
| CVE-2026-20687 | |
| CVE-2026-20688 | |
| CVE-2026-20690 | |
| CVE-2026-20691 | |
| CVE-2026-20692 | |
| CVE-2026-20693 | |
| CVE-2026-20694 | |
| CVE-2026-20695 | |

| | |
|---|---|
| CVE-2026-20697 | |
| CVE-2026-20698 | |
| CVE-2026-20699 | |
| CVE-2026-20701 | |
| CVE-2026-28816 | |
| CVE-2026-28817 | |
| CVE-2026-28818 | |
| CVE-2026-28820 | |
| CVE-2026-28821 | |
| CVE-2026-28822 | |
| CVE-2026-28823 | |
| CVE-2026-28824 | |
| CVE-2026-28825 | |
| CVE-2026-28826 | 4.8 MEDIUM |
| CVE-2026-28827 | 4.8 MEDIUM |
| CVE-2026-28828 | 4.8 MEDIUM |
| CVE-2026-28829 | 4.8 MEDIUM |
| CVE-2026-28831 | 4.8 MEDIUM |
| CVE-2026-28832 | |
| CVE-2026-28833 | 4.8 MEDIUM |
| CVE-2026-28834 | 5.7 MEDIUM |
| CVE-2026-28835 | |
| CVE-2026-28837 | 4.8 MEDIUM |

| | |
|---|---|
| CVE-2026-28838 | 4.8 MEDIUM |
| CVE-2026-28839 | 4.8 MEDIUM |
| CVE-2026-28841 | 5.3 MEDIUM |
| CVE-2026-28842 | 5.3 MEDIUM |
| CVE-2026-28844 | 4.8 MEDIUM |
| CVE-2026-28845 | 4.8 MEDIUM |
| CVE-2026-28852 | 6.8 MEDIUM |
| CVE-2026-28857 | 5.3 MEDIUM |
| CVE-2026-28859 | 5.3 MEDIUM |
| CVE-2026-28861 | 5.3 MEDIUM |
| CVE-2026-28862 | 4.8 MEDIUM |
| CVE-2026-28864 | 4.8 MEDIUM |
| CVE-2026-28865 | 6.3 MEDIUM |
| CVE-2026-28866 | 4.8 MEDIUM |
| CVE-2026-28867 | 4.8 MEDIUM |
| CVE-2026-28868 | 4.8 MEDIUM |
| CVE-2026-28870 | 4.8 MEDIUM |
| CVE-2026-28871 | 5.3 MEDIUM |
| CVE-2026-28876 | 4.8 MEDIUM |
| CVE-2026-28877 | 4.8 MEDIUM |
| CVE-2026-28878 | 4.8 MEDIUM |
| CVE-2026-28879 | 5.3 MEDIUM |
| CVE-2026-28880 | 4.8 MEDIUM |

| | |
|---|---|
| CVE-2026-28881 | 4.8 MEDIUM |
| CVE-2026-28882 | 4.8 MEDIUM |
| CVE-2026-28886 | 2.3 LOW |
| CVE-2026-28888 | 7.3 HIGH |
| CVE-2026-28891 | 2.0 LOW |
| CVE-2026-28892 | 4.8 MEDIUM |
| CVE-2026-28893 | 4.8 MEDIUM |
| CVE-2026-28894 | 8.7 HIGH |

## CWE's

| CWE | Beschrijving |
|---|---|
| CWE-20 | Improper Input Validation |
| CWE-22 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') |
| CWE-77 | Improper Neutralization of Special Elements used in a Command ('Command Injection') |
| CWE-79 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') |
| CWE-119 | Improper Restriction of Operations within the Bounds of a Memory Buffer |
| CWE-122 | Heap-based Buffer Overflow |
| CWE-125 | Out-of-bounds Read |
| CWE-150 | Improper Neutralization of Escape, Meta, or Control Sequences |
| CWE-190 | Integer Overflow or Wraparound |
| CWE-200 | Exposure of Sensitive Information to an Unauthorized Actor |
| CWE-201 | Insertion of Sensitive Information Into Sent Data |
| CWE-265 | Privilege Issues |

| | |
|---|---|
| CWE-275 | Permission Issues |
| CWE-284 | Improper Access Control |
| CWE-285 | Improper Authorization |
| CWE-287 | Improper Authentication |
| CWE-288 | Authentication Bypass Using an Alternate Path or Channel |
| CWE-305 | Authentication Bypass by Primary Weakness |
| CWE-346 | Origin Validation Error |
| CWE-362 | Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') |
| CWE-371 | State Issues |
| CWE-377 | Insecure Temporary File |
| CWE-404 | Improper Resource Shutdown or Release |
| CWE-416 | Use After Free |
| CWE-476 | NULL Pointer Dereference |
| CWE-522 | Insufficiently Protected Credentials |
| CWE-532 | Insertion of Sensitive Information into Log File |
| CWE-601 | URL Redirection to Untrusted Site ('Open Redirect') |
| CWE-918 | Server-Side Request Forgery (SSRF) |
| CWE-942 | Permissive Cross-domain Security Policy with Untrusted Domains |

## Getroffen producten

| **Apple** |
|---|
| Mac<br>OS |

## Disclaimer