Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0140

Kwetsbaarheden verholpen in Apple AirPlay zoals gebruikt door macOS, iOS en iPadOS

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 30-04-2025

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 AirPlay, zoals gebruikt in diverse Apple-producten waaronder macOS, iOS en iPadOS.

Duiding

De kwetsbaarheden worden misbruikt voor het veroorzaken van een Denial-of-Service, het omzeilen van authenticatie en het uitvoeren van willekeurige code. Hiertoe dient de kwaadwillende via AirPlay vanaf een lokaal netwerk malafide content naar een kwetsbaar systeem te sturen.

De kwetsbaarheden zijn ontdekt door onderzoekers van beveiligingsbedrijf Oligo. De onderzoekers geven aan dat de kwetsbaarheden achtereenvolgens kunnen worden misbruikt voor het uitvoeren van malafide code op een systeem, zonder dat hiervoor authenticatie is vereist.

Oplossingen

Apple heeft op 31 maart updates uitgebracht om de kwetsbaarheden te verhelpen in verschillende versies van macOS, iOS en iPadOS. Ook zijn updates uigebracht voor tvOS en AirPlay SDK's. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://support.apple.com/en-us/122371
- https://support.apple.com/en-us/122372
- https://support.apple.com/en-us/122373
- https://support.apple.com/en-us/122374
- https://support.apple.com/en-us/122375
- https://support.apple.com/en-us/122377
- https://support.apple.com/en-us/122403
- https://www.oligo.security/blog/airborne

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-24126	9.8 CRITICAL
CVE-2025-24129	7.5 HIGH

CVE-2025-24131	
CVE-2025-24177	
CVE-2025-24179	
CVE-2025-24206	7.7 HIGH
CVE-2025-24251	5.3 MEDIUM
CVE-2025-24252	9.8 CRITICAL
CVE-2025-24270	5.5 MEDIUM
CVE-2025-24271	6.2 MEDIUM
CVE-2025-30445	5.3 MEDIUM
CVE-2025-31197	5.3 MEDIUM
CVE-2025-31202	7.1 HIGH

CWE's

CWE	Beschrijving
CWE-863	Incorrect Authorization
CWE-416	Use After Free
CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')
CWE-404	Improper Resource Shutdown or Release
CWE-862	Missing Authorization
CWE-476	NULL Pointer Dereference
CWE-400	Uncontrolled Resource Consumption
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Getroffen producten

Apple
AirPlay audio SDK
AirPlay video SDK
CarPlay Communication Plug-in
Iphone Os
iPadOS
macOS
iOS and iPadOS
iPad OS
iPhone OS

Disclaimer