



NCSC-2024-0240

Kwetsbaarheden verholpen in Google Android en Samsung Mobile

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 07-06-2024

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).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Google heeft kwetsbaarheden verholpen in Android.

Duiding

De kwetsbaarheden stellen een kwaadwillende in staat om zich verhoogde rechten toe te kennen, een Denial-of-Service te veroorzaken of toegang te krijgen tot gevoelige gegevens.

Voor succesvol misbruik moet de kwaadwillende het slachtoffer misleiden een malafide link te openen, of een malafide app te installeren en draaien.

In deze updates zijn tevens kwetsbaarheden verholpen in Closed-source componenten van Imagination Technologies, MediaTek en Qualcomm. Google heeft zoals gebruikelijk verder weinig inhoudelijke informatie vrijgegeven.

Oplossingen

Google heeft updates uitgebracht om de kwetsbaarheden te verhelpen in Android 12, 13 en 14.

Samsung heeft updates uitgebracht om de voor Samsung relevante kwetsbaarheden te verhelpen in Samsung Mobile devices.

Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=06>
- <https://source.android.com/docs/security/bulletin/2024-06-01>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2023-21266	
➤ CVE-2023-43538	
➤ CVE-2023-43542	
➤ CVE-2023-43551	

> CVE-2023-43556
> CVE-2024-0671
> CVE-2024-1065
> CVE-2024-20065
> CVE-2024-20066
> CVE-2024-20067
> CVE-2024-20068
> CVE-2024-20069
> CVE-2024-20873
> CVE-2024-20874
> CVE-2024-20875
> CVE-2024-20876
> CVE-2024-20877
> CVE-2024-20878
> CVE-2024-20879
> CVE-2024-20880
> CVE-2024-20881
> CVE-2024-20882
> CVE-2024-20883
> CVE-2024-20884
> CVE-2024-20885
> CVE-2024-23363
> CVE-2024-23696

[> CVE-2024-26926](#)[> CVE-2024-31311](#)[> CVE-2024-31312](#)[> CVE-2024-31313](#)

CWE's

CWE	Beschrijving
> CVE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
> CVE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
> CVE-122	Heap-based Buffer Overflow
> CVE-125	Out-of-bounds Read
> CVE-126	Buffer Over-read
> CVE-1285	Improper Validation of Specified Index, Position, or Offset in Input
> CVE-20	Improper Input Validation
> CVE-200	Exposure of Sensitive Information to an Unauthorized Actor
> CVE-284	Improper Access Control
> CVE-287	Improper Authentication
> CVE-416	Use After Free
> CVE-648	Incorrect Use of Privileged APIs
> CVE-757	Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade')
> CVE-787	Out-of-bounds Write
> CVE-926	Improper Export of Android Application Components

Getroffen producten

google
android
samsung
mobile_devices
mobile_device

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.