



NCSC-2024-0358

Kwetsbaarheden verholpen in Google Android en Samsung Mobile

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 05-09-2024

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

Een kwaadwillende kan de kwetsbaarheden misbruiken om zich verhoogde rechten toe te kennen op het device en zo willekeurige code uit te voeren, mogelijk met rechten van het systeem en toegang krijgen tot gevoelige gegevens.

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

In deze update wordt ook de kwetsbaarheid met kenmerk CVE-2024-32896 verholpen. Deze bevindt zich in het Android Framework en stelt een lokale kwaadwillende in staat om zich verhoogde rechten toe te kennen en code uit te voeren met rechten van het systeem. Van deze kwetsbaarheid meldt Google dat deze zeer beperkt en gericht is misbruikt als ZeroDay op Google Pixel. Er is (nog) geen publieke Proof-of-Concept of exploit beschikbaar.

In deze update zijn ook kwetsbaarheden verholpen in closed-source componenten van Arm, Imagination Technologies, Unisoc en Qualcomm. Google heeft verder weinig inhoudelijke informatie bekend gesteld.

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=09>
- <https://source.android.com/docs/security/bulletin/2024-09-01>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2024-3655	

> CVE-2024-23358	
> CVE-2024-23359	
> CVE-2024-23362	
> CVE-2024-23364	
> CVE-2024-23365	
> CVE-2024-23716	
> CVE-2024-31336	
> CVE-2024-32896	7.8 HIGH
> CVE-2024-33016	
> CVE-2024-33034	
> CVE-2024-33035	
> CVE-2024-33038	
> CVE-2024-33042	
> CVE-2024-33043	
> CVE-2024-33045	
> CVE-2024-33048	
> CVE-2024-33050	
> CVE-2024-33051	
> CVE-2024-33052	
> CVE-2024-33054	
> CVE-2024-33057	
> CVE-2024-33060	
> CVE-2024-34637	

> CVE-2024-34638
> CVE-2024-34640
> CVE-2024-34641
> CVE-2024-34642
> CVE-2024-34643
> CVE-2024-34644
> CVE-2024-34645
> CVE-2024-34646
> CVE-2024-34647
> CVE-2024-34648
> CVE-2024-34649
> CVE-2024-34650
> CVE-2024-34651
> CVE-2024-34652
> CVE-2024-34653
> CVE-2024-34654
> CVE-2024-34655
> CVE-2024-36972
> CVE-2024-39431
> CVE-2024-39432
> CVE-2024-40650
> CVE-2024-40652
> CVE-2024-40654

[> CVE-2024-40655](#)[> CVE-2024-40656](#)[> CVE-2024-40657](#)[> CVE-2024-40658](#)[> CVE-2024-40659](#)[> CVE-2024-40662](#)

CWE's

CWE	Beschrijving
> 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-126	Buffer Over-read
> CWE-190	Integer Overflow or Wraparound
> CWE-20	Improper Input Validation
> CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
> CWE-280	Improper Handling of Insufficient Permissions or Privileges
> CWE-284	Improper Access Control
> CWE-285	Improper Authorization
> CWE-310	CWE-310
> CWE-416	Use After Free
> CWE-476	NULL Pointer Dereference
> CWE-562	Return of Stack Variable Address
> CWE-648	Incorrect Use of Privileged APIs
> CWE-755	Improper Handling of Exceptional Conditions

➤ CWE-822	Untrusted Pointer Dereference
➤ CWE-863	Incorrect Authorization
➤ CWE-926	Improper Export of Android Application Components

Getroffen producten

samsung
mobile_devices
mobile_device
google
android

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.