Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0278

Kwetsbaarheden verholpen in Google Android en Samsung Mobile

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 03-07-2024

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 malafife app te installeren en draaien of een malafide link te volgen.

In deze update zijn ook kwetsbaarheden verholpen in closed-source componenten van Arm, Imagination Technologies, MediaTek 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://source.android.com/docs/security/bulletin/2024-07-01
- https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=07

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-0153	
CVE-2024-4610	
CVE-2024-20076	
CVE-2024-20077	

- CVE-2024-20888
- CVE-2024-20889
- CVE-2024-20890
- CVE-2024-20891
- CVE-2024-20892
- CVE-2024-20893
- CVE-2024-20894
- CVE-2024-20895
- CVE-2024-20896
- CVE-2024-20897
- CVE-2024-20898
- CVE-2024-20899
- CVE-2024-20900
- CVE-2024-20901
- CVE-2024-21460
- CVE-2024-21461
- CVE-2024-21462
- CVE-2024-21465
- CVE-2024-21469
- CVE-2024-23368
- CVE-2024-23372
- CVE-2024-23373
- CVE-2024-23380

- CVE-2024-26923
- CVE-2024-31320
- CVE-2024-31331
- CVE-2024-31332
- CVE-2024-31334
- CVE-2024-31335
- CVE-2024-31339
- CVE-2024-34583
- CVE-2024-34584
- CVE-2024-34585
- CVE-2024-34586
- CVE-2024-34587
- CVE-2024-34588
- CVE-2024-34589
- CVE-2024-34590
- CVE-2024-34591
- CVE-2024-34592
- CVE-2024-34593
- CVE-2024-34594
- CVE-2024-34595
- CVE-2024-34720
- CVE-2024-34721
- CVE-2024-34722

- CVE-2024-34723
- CVE-2024-34724
- CVE-2024-34725
- CVE-2024-34726

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-1288	Improper Validation of Consistency within Input
CWE-190	Integer Overflow or Wraparound
CWE-20	Improper Input Validation
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-264	CWE-264
CWE-269	Improper Privilege Management
CWE-280	Improper Handling of Insufficient Permissions or Privileges
CWE-284	Improper Access Control
CWE-287	Improper Authentication
CWE-330	Use of Insufficiently Random Values
CWE-347	Improper Verification of Cryptographic Signature
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-371	CWE-371
CWE-415	Double Free
CWE-416	Use After Free

CWE-787	Out-of-bounds Write
CWE-927	Use of Implicit Intent for Sensitive Communication

Getroffen producten

google
android
samsung
mobile_devices
mobile_device

Disclaimer