Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0429

Kwetsbaarheden verholpen in Google Android en Samsung Mobile

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 05-11-2024

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. In deze update zijn ook updates meegenomen voor closed-source componenten van Qualcomm, Imagination Technologies en MediaTek.

Samsung heeft kwetsbaarheden in Samsung Mobile verholpen die relevant zijn voor Samsung mobile devices.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om een Denial-of-Service te veroorzaken, zichzelf verhoogde rechten toe te kennen, toegang te krijgen tot gevoelige gegevens of willekeurige code uit te voeren.

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

Van de kwetsbaarheden met kenmerk CVE-2024-43047 en CVE-2024-43093 geeft Google aan, indicaties te hebben dat deze beperkt en gericht zijn misbruikt. Deze kwetsbaarheden bevinden zich respectievelijk in een gesloten component van Qualcomm en de Android Framework.

Google heeft verder zoals gebruikelijk weinig inhoudelijke informatie beschikbaar gesteld.

Oplossingen

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

Samsung heeft updates uitgebracht om kwetsbaarheden die relevant zijn voor Samsung Mobile devices te verhelpen.

Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://source.android.com/docs/security/bulletin/2024-11-01
- https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=11

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-34719	

CVE-2024-34729	
CVE-2024-34747	
CVE-2024-36978	
CVE-2024-38402	
CVE-2024-38403	
CVE-2024-38405	
CVE-2024-38408	
CVE-2024-38415	
CVE-2024-38421	
CVE-2024-38422	
CVE-2024-38423	
CVE-2024-38424	
CVE-2024-40660	
CVE-2024-40661	
CVE-2024-40671	
CVE-2024-43047	
CVE-2024-43080	
CVE-2023-35659	
CVE-2023-35686	
CVE-2024-20104	8.4 HIGH
CVE-2024-20106	6.7 MEDIUM
CVE-2024-21455	
CVE-2024-23385	

- CVE-2024-23715
- CVE-2024-29779 **7.8 HIGH**
- CVE-2024-31337
- CVE-2024-34673
- CVE-2024-34674
- CVE-2024-34675
- CVE-2024-34676
- CVE-2024-34677
- CVE-2024-34678
- CVE-2024-34679
- CVE-2024-34680
- CVE-2024-34681
- CVE-2024-34682
- CVE-2024-43081
- CVE-2024-43082
- CVE-2024-43083
- CVE-2024-43084
- CVE-2024-43085
- CVE-2024-43086
- CVE-2024-43087
- CVE-2024-43088
- CVE-2024-43089
- CVE-2024-43090

- CVE-2024-43091
- CVE-2024-43093
- CVE-2024-45185
- CVE-2024-46740
- CVE-2024-49401
- CVE-2024-49402

CWE's

CWE	Beschrijving
CWE-310	CWE-310
CWE-822	Untrusted Pointer Dereference
CWE-126	Buffer Over-read
CWE-617	Reachable Assertion
CWE-680	Integer Overflow to Buffer Overflow
CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
CWE-416	Use After Free
CWE-787	Out-of-bounds Write
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Getroffen producten

google
android

samsung
devices

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.