Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0039

Kwetsbaarheden verholpen in Google Android en Samsung Mobile

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 04-02-2025

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

Google heeft kwetsbaarheden verholpen in Android. In deze update zijn ook updates meegenomen voor closed-source componenten van Qualcomm, Imagination Technologies, Unisoc en MediaTek.

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

Duiding

De kwetsbaarheden omvatten onder andere lokale informatie openbaarmaking door ongeautoriseerde toegang tot afbeeldingen van andere gebruikers, en een gebrek aan juiste privilegebeheer dat kan leiden tot ongeautoriseerde toegang en controle over apparaten. Deze kwetsbaarheden kunnen worden misbruikt zonder dat er extra uitvoeringsprivileges of gebruikersinteractie nodig zijn, wat de impact op de privacy en gegevensintegriteit van gebruikers aanzienlijk vergroot.

Oplossingen

Google heeft updates uitgebracht om de kwetsbaarheden te verhelpen in Android 12,13,14 en 15.

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

Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=02
- https://source.android.com/docs/security/bulletin/2025-02-01

Kwetsbaarheden

CVE	CVSS Score
CVE-2023-40122	5.3 MEDIUM
CVE-2023-40133	5.5 MEDIUM
CVE-2023-40134	
CVE-2023-40135	3.3 LOW

CVE-2023-40136	
CVE-2023-40137	
CVE-2023-40138	
CVE-2023-40139	5.5 MEDIUM
CVE-2024-0037	3.3 LOW
CVE-2024-20141	6.8 MEDIUM
CVE-2024-20142	6.6 MEDIUM
CVE-2024-38404	7.5 HIGH
CVE-2024-38420	8.8 HIGH
CVE-2024-39441	
CVE-2024-43705	7.8 HIGH
CVE-2024-45569	9.8 CRITICAL
CVE-2024-45571	7.8 HIGH
CVE-2024-45582	7.8 HIGH
CVE-2024-46973	7.8 HIGH
CVE-2024-47892	7.8 HIGH
CVE-2024-49721	
CVE-2024-49723	
CVE-2024-49729	
CVE-2024-49741	
CVE-2024-49743	
CVE-2024-49746	
CVE-2024-49832	7.8 HIGH

CVE-2024-49833	7.8 HIGH
CVE-2024-49834	7.8 HIGH
CVE-2024-49839	8.2 HIGH
CVE-2024-49843	7.8 HIGH
CVE-2024-52935	4.1 MEDIUM
CVE-2024-53104	7.8 HIGH
CVE-2025-0015	7.8 HIGH
CVE-2025-0088	
CVE-2025-0091	
CVE-2025-0094	
CVE-2025-0095	
CVE-2025-0096	
CVE-2025-0097	
CVE-2025-0098	
CVE-2025-0099	
CVE-2025-0100	
CVE-2025-20634	9.8 CRITICAL
CVE-2025-20635	6.8 MEDIUM
CVE-2025-20636	7.8 HIGH
CVE-2025-20904	6.3 MEDIUM
CVE-2025-20905	6.3 MEDIUM
CVE-2025-20906	5.5 MEDIUM
CVE-2025-20907	6.0 MEDIUM

CWE's

CWE	Beschrijving
CWE-123	Write-what-where Condition
CWE-922	Insecure Storage of Sensitive Information
CWE-126	Buffer Over-read
CWE-823	Use of Out-of-range Pointer Offset
CWE-280	Improper Handling of Insufficient Permissions or Privileges
CWE-129	Improper Validation of Array Index
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-862	Missing Authorization
CWE-416	Use After Free
CWE-787	Out-of-bounds Write
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-20	Improper Input Validation

Getroffen producten

google
android
samsung_mobile
samsung_mobile_devices

Disclaimer