Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0072

Kwetsbaarheden verholpen in Google Android en Samsung Mobile

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 04-03-2025

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 meerdere kwetsbaarheden verholpen in Android en Samsung Mobile, waaronder twee zero-day kwetsbaarheden die actief werden uitgebuit in gerichte aanvallen.

Duiding

De kwetsbaarheden bevinden zich in de Android-kernel en de ExternalStorageProvider.java, wat kan leiden tot lokale privilege-escalatie en remote code-executie. Daarnaast kunnen verschillende kwetsbaarheden remote aanvallers in staat stellen om denial-of-service te veroorzaken of gevoelige gegevens te benaderen. De kwetsbaarheden treffen verschillende versies van Android en Samsung-producten, wat onmiddellijke aandacht van beveiligingsbeheerders vereist.

Google meldt informatie te hebben ontvangen dat de kwetsbaarheden met kenmerk CVE-2024-43093 en CVE-2024-50302 beperkt en gericht zijn misbruikt. Deze kwetsbaarheden bevinden zich respectievelijk in het Android Framework en in de Kernel en stellen een kwaadwillende in staat zich verhoogde rechten toe te kennen en toegang te krijgen tot gevoelige gegevens. Voor zover bekend moet voor succesvol misbruik de kwaadwillende het slachtoffer misleiden een malafide app te installeren.

Oplossingen

Google heeft fixes geïmplementeerd om deze risico's te mitigeren, terwijl Samsung soortgelijke problemen in zijn apparaten heeft aangepakt. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://source.android.com/docs/security/bulletin/2025-03-01
- https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=03

Kwetsbaarheden

CVE	CVSS Score
CVE-2023-21125	
CVE-2024-43051	4.8 MEDIUM
CVE-2024-43093	7.8 HIGH
CVE-2024-46852	5.1 MEDIUM

CVE-2024-49728	
CVE-2024-49836	8.5 HIGH
CVE-2024-49838	8.2 HIGH
CVE-2024-50302	5.1 MEDIUM
CVE-2024-53011	4.6 MEDIUM
CVE-2024-53014	8.5 HIGH
CVE-2024-53024	8.5 HIGH
CVE-2024-53025	6.8 MEDIUM
CVE-2024-53027	8.7 HIGH
CVE-2025-0074	
CVE-2025-0075	
CVE-2025-0079	
CVE-2025-0081	
CVE-2025-0082	
CVE-2025-0084	
CVE-2025-0092	
CVE-2025-0093	
CVE-2025-20644	6.3 MEDIUM
CVE-2025-20645	4.6 MEDIUM
CVE-2025-20903	
CVE-2025-20908	
CVE-2025-20909	
CVE-2025-20910	

- CVE-2025-20911
- CVE-2025-20912
- CVE-2025-22403
- CVE-2025-22404
- CVE-2025-22405
- CVE-2025-22406
- CVE-2025-22407
- CVE-2025-22408
- CVE-2025-22409
- CVE-2025-22410
- CVE-2025-22411
- CVE-2025-22412
- CVE-2025-22413
- CVE-2025-26417

CWE's

CWE	Beschrijving
CWE-264	CWE-264
CWE-126	Buffer Over-read
CWE-193	Off-by-one Error
CWE-1286	Improper Validation of Syntactic Correctness of Input
CWE-908	Use of Uninitialized Resource
CWE-129	Improper Validation of Array Index
CWE-190	Integer Overflow or Wraparound

CWE-665	Improper Initialization
CWE-285	Improper Authorization
CWE-476	NULL Pointer Dereference
CWE-787	Out-of-bounds Write
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Getroffen producten

Android
System
Samsung
Mobile Devices

Disclaimer