Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0143

Kwetsbaarheden verholpen in Google Android en Samsung Mobile

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 07-05-2025

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.

Duiding

De kwetsbaarheden bevinden zich onderandere in de Keymaster trustlet, SmartManagerCN en FreeType. De kwetsbaarheden stellen een lokale aanvaller in staat om code uit te voeren op het apparaat en code uit te voeren met de rechten van SmartManagerCN. Google meldt informatie te hebben ontvangen dat de kwetsbaarheid met kenmerk CVE-2025-27363 beperkt en gericht als zeroday is misbruikt. Deze kwetsbaarheid bevindt zich in FreeType en stelt een kwaadwillende in staat code uit te voeren middels een heap buffer overflow.

Oplossingen

Google heeft updates uitgebracht om de kwetsbaarheden te verhelpen in Android 12,13, 14 en 15. 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/2025-05-01
- https://source.android.com/docs/security/bulletin/2025-05-01
- https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=03

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-26430	
CVE-2025-26435	
CVE-2025-26436	
CVE-2025-26438	
CVE-2025-26440	
CVE-2025-26442	

CVE-2025-26444	
CVE-2025-27363	6.3 MEDIUM
CVE-2025-0072	8.5 HIGH
CVE-2025-0077	
CVE-2025-0087	
CVE-2025-0427	8.5 HIGH
CVE-2023-21342	7.8 HIGH
CVE-2023-35657	
CVE-2024-12577	8.5 HIGH
CVE-2024-34739	4.8 MEDIUM
CVE-2024-45580	8.7 HIGH
CVE-2024-46974	5.1 MEDIUM
CVE-2024-46975	8.5 HIGH
CVE-2024-47891	8.6 HIGH
CVE-2024-47896	8.5 HIGH
CVE-2024-47900	5.1 MEDIUM
CVE-2024-49739	
CVE-2024-49835	8.5 HIGH
CVE-2024-49841	8.5 HIGH
CVE-2024-49842	8.5 HIGH
CVE-2024-49845	8.5 HIGH
CVE-2024-49846	6.9 MEDIUM
CVE-2024-49847	8.7 HIGH

CVE-2024-52939	8.5 HIGH
CVE-2025-20666	8.7 HIGH
CVE-2025-21453	8.5 HIGH
CVE-2025-21459	8.7 HIGH
CVE-2025-21467	8.5 HIGH
CVE-2025-21468	8.5 HIGH
CVE-2025-22425	
CVE-2025-26420	
CVE-2025-26421	
CVE-2025-26422	
CVE-2025-26423	
CVE-2025-26424	
CVE-2025-26425	
CVE-2025-26426	
CVE-2025-26427	
CVE-2025-26428	
CVE-2025-26429	

CWE's

CWE	Beschrijving
CWE-390	Detection of Error Condition Without Action
CWE-274	Improper Handling of Insufficient Privileges
CWE-126	Buffer Over-read
CWE-823	Use of Out-of-range Pointer Offset

CWE-270	Privilege Context Switching Error
CWE-266	Incorrect Privilege Assignment
CWE-617	Reachable Assertion
CWE-116	Improper Encoding or Escaping of Output
CWE-284	Improper Access Control
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
CWE-416	Use After Free
CWE-863	Incorrect Authorization
CWE-787	Out-of-bounds Write
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-269	Improper Privilege Management
CWE-20	Improper Input Validation
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

Android
System
Framework
Samsung
Samsung Mobile

Disclaimer