Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0273

Kwetsbaarheden verholpen in Google Android en Samsung Mobile

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 04-09-2025

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. Samsung heeft de voor Samsung Mobile relevante kwetsbaarheden verholpen in Samsung Mobile.

Duiding

De kwetsbaarheden in de Android kernel omvatten onder andere een raceconditie tussen functies die CPU-timers beheren, wat kan leiden tot systeeminstabiliteit. Daarnaast zijn er kwetsbaarheden gerapporteerd die ongeautoriseerde toegang tot gevoelige informatie mogelijk maken door onjuist gebruik van geheugen en systeemoproepen. Dit kan resulteren in ernstige beveiligingsimplicaties, waaronder het uitvoeren van ongewenste code en het compromitteren van systeemintegriteit.

Naast kwetsbaarheden in Android zijn ook kwetsbaarheden verholpen in Closed-source componenten van Arm, Mediatek, Imagination Technologies en Qualcomm.

Google meldt informatie te hebben ontvangen dat de kwetsbaarheden met kenmerk CVE-2025-38352 en CVE-2025-48543 beperkt en gericht zijn misbruikt. Er is geen publieke Proof-of-Concept-code of exploit bekend van deze kwetsbaarheden.

Oplossingen

Google heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Samsung heeft updates uitgebracht om de voor Samsung Mobile relevante kwetsbaarheden te verhelpen.

Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=09
- https://source.android.com/docs/security/bulletin/2025-09-01

Kwetsbaarheden

CVE	CVSS Score
CVE-2021-39810	7.8 HIGH
CVE-2023-24023	6.8 MEDIUM
CVE-2024-7881	2.0 LOW

CVE-2024-47898	8.6 HIGH
CVE-2024-47899	8.6 HIGH
CVE-2024-49714	
CVE-2025-0076	
CVE-2025-0089	
CVE-2025-0467	8.6 HIGH
CVE-2025-1246	8.5 HIGH
CVE-2025-1706	8.5 HIGH
CVE-2025-3212	
CVE-2025-8109	8.8 HIGH
CVE-2025-20696	7.0 HIGH
CVE-2025-20703	8.7 HIGH
CVE-2025-20704	9.3 CRITICAL
CVE-2025-20708	9.3 CRITICAL
CVE-2025-21025	4.8 MEDIUM
CVE-2025-21026	4.8 MEDIUM
CVE-2025-21027	4.8 MEDIUM
CVE-2025-21028	4.8 MEDIUM
CVE-2025-21029	4.8 MEDIUM
CVE-2025-21030	2.4 LOW
CVE-2025-21031	4.8 MEDIUM
CVE-2025-21032	2.4 LOW
CVE-2025-21033	4.8 MEDIUM

CVE-2025-21034	4.8 MEDIUM
CVE-2025-21427	6.9 MEDIUM
CVE-2025-21432	8.5 HIGH
CVE-2025-21433	6.8 MEDIUM
CVE-2025-21446	8.7 HIGH
CVE-2025-21449	8.7 HIGH
CVE-2025-21450	6.9 MEDIUM
CVE-2025-21454	8.7 HIGH
CVE-2025-21464	4.8 MEDIUM
CVE-2025-21465	4.8 MEDIUM
CVE-2025-21477	8.7 HIGH
CVE-2025-21481	
CVE-2025-21482	
CVE-2025-21483	
CVE-2025-21484	
CVE-2025-21487	
CVE-2025-21488	
CVE-2025-21755	6.9 MEDIUM
CVE-2025-25179	8.6 HIGH
CVE-2025-25180	8.5 HIGH
CVE-2025-26454	
CVE-2025-26464	
CVE-2025-27032	

CVE-2025-27034	
CVE-2025-27042	8.5 HIGH
CVE-2025-27043	8.5 HIGH
CVE-2025-27052	8.5 HIGH
CVE-2025-27056	8.5 HIGH
CVE-2025-27057	8.7 HIGH
CVE-2025-27061	8.5 HIGH
CVE-2025-27065	8.7 HIGH
CVE-2025-27066	8.7 HIGH
CVE-2025-27073	8.7 HIGH
CVE-2025-32321	
CVE-2025-32323	
CVE-2025-32324	
CVE-2025-32325	
CVE-2025-32326	
CVE-2025-32327	
CVE-2025-32330	
CVE-2025-32331	
CVE-2025-32332	
CVE-2025-32333	
CVE-2025-32345	
CVE-2025-32346	
CVE-2025-32347	

CVE-2025-32349	
CVE-2025-32350	
CVE-2025-38352	2.1 LOW
CVE-2025-46707	5.2 MEDIUM
CVE-2025-46708	8.6 HIGH
CVE-2025-46710	8.5 HIGH
CVE-2025-47317	
CVE-2025-47318	
CVE-2025-47326	
CVE-2025-47328	
CVE-2025-47329	
CVE-2025-48522	
CVE-2025-48523	
CVE-2025-48524	
CVE-2025-48526	
CVE-2025-48527	
CVE-2025-48528	
CVE-2025-48529	
CVE-2025-48531	
CVE-2025-48532	
CVE-2025-48534	
CVE-2025-48535	
CVE-2025-48537	

- CVE-2025-48538
- CVE-2025-48539
- CVE-2025-48540
- CVE-2025-48541
- CVE-2025-48542
- CVE-2025-48543
- CVE-2025-48544
- CVE-2025-48545
- CVE-2025-48546
- CVE-2025-48547
- CVE-2025-48548
- CVE-2025-48549
- CVE-2025-48550
- CVE-2025-48551
- CVE-2025-48552
- CVE-2025-48553
- CVE-2025-48554
- CVE-2025-48556
- CVE-2025-48558
- CVE-2025-48559
- CVE-2025-48560
- CVE-2025-48561
- CVE-2025-48562

- CVE-2025-48563
- CVE-2025-48581

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
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-125	Out-of-bounds Read
CWE-126	Buffer Over-read
CWE-129	Improper Validation of Array Index
CWE-131	Incorrect Calculation of Buffer Size
CWE-142	Improper Neutralization of Value Delimiters
CWE-280	Improper Handling of Insufficient Permissions or Privileges
CWE-284	Improper Access Control
CWE-287	Improper Authentication
CWE-300	Channel Accessible by Non-Endpoint
CWE-326	Inadequate Encryption Strength
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
CWE-371	CWE-371
CWE-404	Improper Resource Shutdown or Release
CWE-415	Double Free
CWE-416	Use After Free
CWE-476	NULL Pointer Dereference
CWE-617	Reachable Assertion

CWE-668	Exposure of Resource to Wrong Sphere
CWE-787	Out-of-bounds Write
CWE-823	Use of Out-of-range Pointer Offset
CWE-862	Missing Authorization
CWE-863	Incorrect Authorization
CWE-1422	Exposure of Sensitive Information caused by Incorrect Data Forwarding during Transient Execution

Getroffen producten

Google
Android
Samsung
Samsung Mobile Devices

Disclaimer