Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0074

Kwetsbaarheden verholpen in Google Android en Samsung Mobile

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 03-03-2026

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

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 om een malafide app te installeren en uit te voeren, of een malafide link te volgen.

Google heeft verder, zoals gebruikelijk, weinig inhoudelijke informatie beschikbaar gesteld.

Oplossingen

Google heeft updates uitgebracht om de kwetsbaarheden te verhelpen in Android 14, 15 en 16.

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/2026/2026-03-01
- https://security.samsungmobile.com//securityUpdate.smsb

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-43766	6.5 MEDIUM
CVE-2024-43859	5.5 MEDIUM
CVE-2025-2879	4.8 MEDIUM

CVE-2025-10865	7.8 HIGH
CVE-2025-13952	5.3 MEDIUM
CVE-2025-20760	6.5 MEDIUM
CVE-2025-20761	6.5 MEDIUM
CVE-2025-20762	6.5 MEDIUM
CVE-2025-20793	6.5 MEDIUM
CVE-2025-20794	8.7 HIGH
CVE-2025-20795	8.4 HIGH
CVE-2025-32313	8.4 HIGH
CVE-2025-38616	5.1 MEDIUM
CVE-2025-38618	8.6 HIGH
CVE-2025-39682	7.1 HIGH
CVE-2025-39946	2.1 LOW
CVE-2025-40266	7.1 HIGH
CVE-2025-47339	7.8 HIGH
CVE-2025-47346	7.8 HIGH
CVE-2025-47348	7.8 HIGH
CVE-2025-47366	7.1 HIGH
CVE-2025-47378	7.1 HIGH
CVE-2025-47385	7.8 HIGH
CVE-2025-47388	7.8 HIGH
CVE-2025-47394	7.8 HIGH
CVE-2025-47395	6.5 MEDIUM

CVE-2025-47396	7.8 HIGH
CVE-2025-47397	7.8 HIGH
CVE-2025-47398	7.8 HIGH
CVE-2025-47402	6.5 MEDIUM
CVE-2025-48544	6.9 MEDIUM
CVE-2025-48567	7.8 HIGH
CVE-2025-48568	7.4 HIGH
CVE-2025-48574	8.4 HIGH
CVE-2025-48577	7.4 HIGH
CVE-2025-48578	7.8 HIGH
CVE-2025-48579	8.4 HIGH
CVE-2025-48582	8.4 HIGH
CVE-2025-48585	6.2 MEDIUM
CVE-2025-48587	6.2 MEDIUM
CVE-2025-48602	
CVE-2025-48605	
CVE-2025-48609	
CVE-2025-48613	
CVE-2025-48619	
CVE-2025-48630	
CVE-2025-48631	7.5 HIGH
CVE-2025-48634	
CVE-2025-48635	

CVE-2025-48641	
CVE-2025-48642	
CVE-2025-48644	
CVE-2025-48645	
CVE-2025-48646	7.8 HIGH
CVE-2025-48650	8.4 HIGH
CVE-2025-48653	
CVE-2025-48654	
CVE-2025-58407	7.4 HIGH
CVE-2025-58408	5.1 MEDIUM
CVE-2025-58409	3.5 LOW
CVE-2025-58411	8.8 HIGH
CVE-2025-59600	7.8 HIGH
CVE-2025-64783	7.8 HIGH
CVE-2025-64784	7.1 HIGH
CVE-2025-64893	7.1 HIGH
CVE-2025-69278	
CVE-2025-69279	
CVE-2026-0005	4.8 MEDIUM
CVE-2026-0006	6.9 MEDIUM
CVE-2026-0007	4.8 MEDIUM
CVE-2026-0008	4.8 MEDIUM
CVE-2026-0010	4.8 MEDIUM

CVE-2026-0011	4.8 MEDIUM
CVE-2026-0012	
CVE-2026-0013	4.8 MEDIUM
CVE-2026-0014	4.8 MEDIUM
CVE-2026-0015	4.8 MEDIUM
CVE-2026-0017	4.8 MEDIUM
CVE-2026-0020	4.8 MEDIUM
CVE-2026-0021	4.8 MEDIUM
CVE-2026-0023	4.8 MEDIUM
CVE-2026-0024	4.8 MEDIUM
CVE-2026-0025	4.8 MEDIUM
CVE-2026-0026	4.8 MEDIUM
CVE-2026-0027	8.4 HIGH
CVE-2026-0028	4.8 MEDIUM
CVE-2026-0029	4.8 MEDIUM
CVE-2026-0030	4.8 MEDIUM
CVE-2026-0031	4.8 MEDIUM
CVE-2026-0032	4.8 MEDIUM
CVE-2026-0034	4.8 MEDIUM
CVE-2026-0035	4.8 MEDIUM
CVE-2026-0037	4.8 MEDIUM
CVE-2026-0038	4.8 MEDIUM
CVE-2026-0047	4.8 MEDIUM

CVE-2026-20401	6.3 MEDIUM
CVE-2026-20402	6.3 MEDIUM
CVE-2026-20403	6.3 MEDIUM
CVE-2026-20404	6.3 MEDIUM
CVE-2026-20405	6.3 MEDIUM
CVE-2026-20406	6.3 MEDIUM
CVE-2026-20420	6.3 MEDIUM
CVE-2026-20421	6.3 MEDIUM
CVE-2026-20422	6.3 MEDIUM
CVE-2026-20425	8.5 HIGH
CVE-2026-20426	8.5 HIGH
CVE-2026-20427	8.5 HIGH
CVE-2026-20428	8.5 HIGH
CVE-2026-20434	6.9 MEDIUM
CVE-2026-20988	
CVE-2026-20989	
CVE-2026-20990	
CVE-2026-20991	
CVE-2026-20992	
CVE-2026-21385	7.8 HIGH
CVE-2026-21735	

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-59	Improper Link Resolution Before File Access ('Link Following')
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
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-121	Stack-based Buffer Overflow
CWE-122	Heap-based Buffer Overflow
CWE-125	Out-of-bounds Read
CWE-126	Buffer Over-read
CWE-190	Integer Overflow or Wraparound
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-275	CWE-275
CWE-280	Improper Handling of Insufficient Permissions or Privileges
CWE-319	Cleartext Transmission of Sensitive Information
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-366	Race Condition within a Thread
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
CWE-400	Uncontrolled Resource Consumption
CWE-401	Missing Release of Memory after Effective Lifetime
CWE-404	Improper Resource Shutdown or Release
CWE-415	Double Free

CWE-416	Use After Free
CWE-441	Unintended Proxy or Intermediary ('Confused Deputy')
CWE-457	Use of Uninitialized Variable
CWE-476	NULL Pointer Dereference
CWE-497	Exposure of Sensitive System Information to an Unauthorized Control Sphere
CWE-617	Reachable Assertion
CWE-639	Authorization Bypass Through User-Controlled Key
CWE-749	Exposed Dangerous Method or Function
CWE-754	Improper Check for Unusual or Exceptional Conditions
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-787	Out-of-bounds Write
CWE-862	Missing Authorization
CWE-1262	Improper Access Control for Register Interface

Getroffen producten

Google
Android
Samsung
Mobile Devices

Disclaimer