Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0185

Kwetsbaarheden verholpen in Google Android en Samsung Mobile

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 10-06-2025

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 het Android besturingssysteem. Samsung heeft de voor Samsung Mobile relevante kwetsbaarheden verholpen in Samsung Mobile.

Duiding

De kwetsbaarheden bevinden zich in de wijze waarop de GPU Kernel Drivers omgaan met systeemoproepen van niet-geprivilegieerde gebruikers. Dit kan leiden tot ongeautoriseerde toegang tot geheugen, geheugenmanipulatie en systeeminstabiliteit. Aangevallen systemen kunnen onvoorspelbaar gedrag vertonen of vastlopen, wat een significante impact heeft op de integriteit en vertrouwelijkheid van gegevens. De kwetsbaarheden zijn vooral zorgwekkend in omgevingen waar gebruikersprivileges niet strikt worden gehandhaafd.

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://source.android.com/docs/security/bulletin/2025-06-01
- https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=06

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-12576	4.8 MEDIUM
CVE-2024-12837	8.5 HIGH
CVE-2024-47893	8.5 HIGH
CVE-2024-53010	8.5 HIGH
CVE-2024-53019	6.9 MEDIUM
CVE-2024-53020	6.9 MEDIUM

CVE-2024-53021	6.9 MEDIUM
CVE-2024-53026	6.9 MEDIUM
CVE-2025-0073	8.5 HIGH
CVE-2025-0468	
CVE-2025-0478	7.8 HIGH
CVE-2025-0819	8.5 HIGH
CVE-2025-0835	7.8 HIGH
CVE-2025-20981	4.8 MEDIUM
CVE-2025-20984	4.8 MEDIUM
CVE-2025-20985	4.8 MEDIUM
CVE-2025-20986	4.8 MEDIUM
CVE-2025-20987	1.8 LOW
CVE-2025-20988	4.8 MEDIUM
CVE-2025-20989	1.8 LOW
CVE-2025-20991	4.8 MEDIUM
CVE-2025-20992	4.8 MEDIUM
CVE-2025-20993	4.8 MEDIUM
CVE-2025-21424	8.5 HIGH
CVE-2025-21485	8.5 HIGH
CVE-2025-21486	8.5 HIGH
CVE-2025-25178	7.8 HIGH
CVE-2025-26432	
CVE-2025-26437	

CVE-2025-26441	
CVE-2025-26443	
CVE-2025-26445	
CVE-2025-26448	
CVE-2025-26449	
CVE-2025-26450	
CVE-2025-26452	
CVE-2025-26453	
CVE-2025-26455	
CVE-2025-26456	
CVE-2025-26458	
CVE-2025-26462	
CVE-2025-26463	
CVE-2025-27029	8.7 HIGH
CVE-2025-32312	

CWE's

CWE	Beschrijving
CWE-1284	Improper Validation of Specified Quantity in Input
CWE-822	Untrusted Pointer Dereference
CWE-126	Buffer Over-read
CWE-823	Use of Out-of-range Pointer Offset
CWE-280	Improper Handling of Insufficient Permissions or Privileges
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition

CWE-284	Improper Access Control
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
CWE-416	Use After Free
CWE-926	Improper Export of Android Application Components
CWE-125	Out-of-bounds Read
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-122	Heap-based Buffer Overflow
CWE-269	Improper Privilege Management
CWE-276	Incorrect Default Permissions

Getroffen producten

Google
Android
Samsung
Android

Disclaimer