Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0379

Kwetsbaarheden verholpen in Google Android en Samsung Mobile

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 02-12-2025

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 zijn voornamelijk gerelateerd aan onjuiste invoervalidatie, wat kan resulteren in systeemcrashes en remote denial of service-aanvallen via kwaadaardige basisstations zonder dat gebruikersinteractie vereist is. Dit vormt een risico voor de stabiliteit en integriteit van de systemen die deze technologie gebruiken.

Google meldt informatie te hebben ontvangen dat de kwetsbaarheden met kenmerk CVE-2025-48633 en CVE-2025-48572 beperkt en gericht zijn misbruikt. Deze kwetsbaarheden bevinden zich in het Android Framework 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 en Samsung hebben patches uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=12
- https://source.android.com/docs/security/bulletin/2025-12-01

Kwetsbaarheden

CVE	CVSS Score
CVE-2023-40130	7.8 HIGH
CVE-2024-35970	6.3 MEDIUM
CVE-2025-3012	8.7 HIGH
CVE-2025-6349	8.5 HIGH

CVE-2025-6573	5.3 MEDIUM
CVE-2025-8045	8.5 HIGH
CVE-2025-11131	8.7 HIGH
CVE-2025-11132	8.7 HIGH
CVE-2025-11133	8.7 HIGH
CVE-2025-20725	7.5 HIGH
CVE-2025-20726	7.5 HIGH
CVE-2025-20727	7.5 HIGH
CVE-2025-20730	6.7 MEDIUM
CVE-2025-20750	
CVE-2025-20751	
CVE-2025-20752	
CVE-2025-20753	
CVE-2025-20754	
CVE-2025-20755	
CVE-2025-20756	
CVE-2025-20757	
CVE-2025-20758	
CVE-2025-20759	
CVE-2025-20790	
CVE-2025-20791	
CVE-2025-20792	
CVE-2025-21072	5.7 MEDIUM

CVE-2025-21080	6.2 MEDIUM
CVE-2025-22420	
CVE-2025-22432	
CVE-2025-25177	8.5 HIGH
CVE-2025-27053	8.5 HIGH
CVE-2025-27054	8.5 HIGH
CVE-2025-27070	7.8 HIGH
CVE-2025-27074	8.8 HIGH
CVE-2025-31717	8.7 HIGH
CVE-2025-31718	9.3 CRITICAL
CVE-2025-32319	
CVE-2025-32328	
CVE-2025-32329	
CVE-2025-38236	8.6 HIGH
CVE-2025-38349	8.6 HIGH
CVE-2025-38500	7.8 HIGH
CVE-2025-46711	6.8 MEDIUM
CVE-2025-47319	
CVE-2025-47323	
CVE-2025-47351	8.5 HIGH
CVE-2025-47354	8.5 HIGH
CVE-2025-47370	6.5 MEDIUM
CVE-2025-47372	

- CVE-2025-47382
- CVE-2025-48525
- CVE-2025-48536
- CVE-2025-48555
- CVE-2025-48564
- CVE-2025-48565
- CVE-2025-48566
- CVE-2025-48572
- CVE-2025-48573
- CVE-2025-48575
- CVE-2025-48576
- CVE-2025-48580
- CVE-2025-48583
- CVE-2025-48584
- CVE-2025-48586
- CVE-2025-48588
- CVE-2025-48589
- CVE-2025-48590
- CVE-2025-48591
- CVE-2025-48592
- CVE-2025-48594
- CVE-2025-48596
- CVE-2025-48597

- CVE-2025-48598
- CVE-2025-48599
- CVE-2025-48600
- CVE-2025-48601
- CVE-2025-48603
- CVE-2025-48604
- CVE-2025-48607
- CVE-2025-48610
- CVE-2025-48612
- CVE-2025-48614
- CVE-2025-48615
- CVE-2025-48617
- CVE-2025-48618
- CVE-2025-48620
- CVE-2025-48621
- CVE-2025-48622
- CVE-2025-48623
- CVE-2025-48624
- CVE-2025-48626
- CVE-2025-48627
- CVE-2025-48628
- CVE-2025-48629
- CVE-2025-48631

CVE-2025-48632	
CVE-2025-48633	
CVE-2025-48637	
CVE-2025-48638	
CVE-2025-48639	
CVE-2025-58410	7.5 HIGH
CVE-2025-58475	5.6 MEDIUM
CVE-2025-58476	4.2 MEDIUM
CVE-2025-58477	4.3 MEDIUM
CVE-2025-58478	4.3 MEDIUM
CVE-2025-58479	4.3 MEDIUM
CVE-2025-58480	4.3 MEDIUM
CVE-2025-61607	8.7 HIGH
CVE-2025-61608	8.7 HIGH
CVE-2025-61609	8.7 HIGH
CVE-2025-61610	8.7 HIGH
CVE-2025-61617	8.7 HIGH
CVE-2025-61618	8.7 HIGH
CVE-2025-61619	8.7 HIGH

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation

CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-122	Heap-based Buffer Overflow
CWE-125	Out-of-bounds Read
CWE-131	Incorrect Calculation of Buffer Size
CWE-190	Integer Overflow or Wraparound
CWE-248	Uncaught Exception
CWE-280	Improper Handling of Insufficient Permissions or Privileges
CWE-287	Improper Authentication
CWE-404	Improper Resource Shutdown or Release
CWE-416	Use After Free
CWE-476	NULL Pointer Dereference
CWE-617	Reachable Assertion
CWE-667	Improper Locking
CWE-769	DEPRECATED: Uncontrolled File Descriptor Consumption
CWE-787	Out-of-bounds Write
CWE-825	Expired Pointer Dereference
CWE-1287	Improper Validation of Specified Type of Input

Getroffen producten

Google
Android
Samsung
Samsung Mobile Devices

Disclaimer