Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0467

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Google Android en Samsung Mobile

Publicatiedatum: 05-11-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Google heeft kwetsbaarheden verholpen in Android.

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

Duiding

De ernstige kwetsbaarheden betreffen onder andere mogelijkheden voor het uitvoeren van willekeurige code op afstand (Remote Code Execution) en het verkrijgen van verhoogde systeemrechten (Privilege Escalation). Hierdoor kunnen aanvallers ongeautoriseerde toegang krijgen tot systeemonderdelen en de controle over het apparaat verkrijgen. Er zijn op dit moment geen berichten bekend over actief misbruik van deze kwetsbaarheden.

Oplossingen

Google heeft beveiligingsupdates uitgebracht om de kwetsbaarheden in Android-versies 14, 15, 16 en 17 te verhelpen.

Samsung heeft daarnaast beveiligingsupdates beschikbaar gesteld om de relevante kwetsbaarheden in Samsung Galaxy-apparaten te verhelpen.

Raadpleeg de onderstaande referenties voor meer informatie en de beschikbare beveiligingsupdates.

Referenties

- https://security.samsungmobile.com/securityUpdate.smsb
- https://source.android.com/docs/security/bulletin/2026/2026-11-01

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-0647	7.9 HIGH
CVE-2025-22424	7.8 HIGH
CVE-2025-22426	7.8 HIGH
CVE-2025-22436	8.4 HIGH
CVE-2025-22442	7.0 HIGH
CVE-2025-26433	8.4 HIGH
CVE-2025-38627	7.3 HIGH
CVE-2025-48600	5.5 MEDIUM
CVE-2026-0053	8.4 HIGH
CVE-2026-6726	8.5 HIGH
CVE-2026-9034	7.8 HIGH
CVE-2026-9040	7.7 HIGH
CVE-2026-11891	5.1 MEDIUM
CVE-2026-15466	
CVE-2026-16280	9.8 CRITICAL
CVE-2026-18629	
CVE-2026-19199	
CVE-2026-20499	7.5 HIGH
CVE-2026-20519	7.5 HIGH
CVE-2026-20520	7.5 HIGH
CVE-2026-20521	8.4 HIGH
CVE-2026-20522	8.4 HIGH
CVE-2026-20523	8.4 HIGH
CVE-2026-20524	8.4 HIGH
CVE-2026-20525	5.3 MEDIUM
CVE-2026-20526	7.1 HIGH
CVE-2026-20527	5.3 MEDIUM
CVE-2026-20545	7.5 HIGH

CVE	CVSS Score
CVE-2026-20546	7.5 HIGH
CVE-2026-20547	7.5 HIGH
CVE-2026-20548	7.5 HIGH
CVE-2026-20549	7.5 HIGH
CVE-2026-20553	6.8 MEDIUM
CVE-2026-20554	7.1 HIGH
CVE-2026-20555	5.3 MEDIUM
CVE-2026-20556	7.5 HIGH
CVE-2026-20557	7.5 HIGH
CVE-2026-20558	8.4 HIGH
CVE-2026-20559	7.8 HIGH
CVE-2026-20560	5.3 MEDIUM
CVE-2026-20561	5.3 MEDIUM
CVE-2026-20562	5.3 MEDIUM
CVE-2026-20563	5.3 MEDIUM
CVE-2026-20564	6.2 MEDIUM
CVE-2026-20565	8.4 HIGH
CVE-2026-20586	8.8 HIGH
CVE-2026-20589	6.7 MEDIUM
CVE-2026-22165	8.1 HIGH
CVE-2026-23184	7.8 HIGH
CVE-2026-23240	7.3 HIGH
CVE-2026-25285	
CVE-2026-25286	
CVE-2026-25287	
CVE-2026-25291	7.8 HIGH
CVE-2026-25301	
CVE-2026-25302	7.1 HIGH
CVE-2026-28580	7.8 HIGH
CVE-2026-28586	3.3 LOW
CVE-2026-28588	8.4 HIGH

CVE	CVSS Score
CVE-2026-28597	8.4 HIGH
CVE-2026-28621	
CVE-2026-28632	4.0 MEDIUM
CVE-2026-28643	6.2 MEDIUM
CVE-2026-28645	6.8 MEDIUM
CVE-2026-28665	8.4 HIGH
CVE-2026-31533	9.8 CRITICAL
CVE-2026-41155	5.5 MEDIUM
CVE-2026-43284	8.8 HIGH
CVE-2026-43499	8.5 HIGH
CVE-2026-45199	7.8 HIGH
CVE-2026-45201	7.8 HIGH
CVE-2026-45204	5.5 MEDIUM
CVE-2026-45514	8.4 HIGH
CVE-2026-45522	
CVE-2026-46232	8.1 HIGH
CVE-2026-46242	7.3 HIGH
CVE-2026-49912	4.0 MEDIUM
CVE-2026-49922	8.4 HIGH
CVE-2026-49923	8.4 HIGH
CVE-2026-49924	6.2 MEDIUM
CVE-2026-49925	
CVE-2026-49931	8.4 HIGH
CVE-2026-49934	7.8 HIGH
CVE-2026-49935	4.0 MEDIUM
CVE-2026-53256	7.7 HIGH
CVE-2026-55257	8.4 HIGH
CVE-2026-55261	8.4 HIGH
CVE-2026-55262	8.4 HIGH
CVE-2026-55263	8.4 HIGH
CVE-2026-55264	4.0 MEDIUM

CVE	CVSS Score
CVE-2026-55271	8.4 HIGH
CVE-2026-55272	6.2 MEDIUM
CVE-2026-55275	8.4 HIGH
CVE-2026-55283	8.4 HIGH
CVE-2026-55287	8.4 HIGH
CVE-2026-55288	8.4 HIGH
CVE-2026-55289	8.4 HIGH
CVE-2026-55292	5.3 MEDIUM
CVE-2026-57537	7.8 HIGH
CVE-2026-57545	7.8 HIGH
CVE-2026-57546	7.5 HIGH
CVE-2026-57547	
CVE-2026-57548	
CVE-2026-57549	
CVE-2026-57554	7.8 HIGH
CVE-2026-58814	7.5 HIGH
CVE-2026-58817	6.2 MEDIUM
CVE-2026-58821	6.2 MEDIUM
CVE-2026-58824	8.4 HIGH
CVE-2026-58825	8.4 HIGH
CVE-2026-58826	8.4 HIGH
CVE-2026-58827	8.4 HIGH
CVE-2026-58828	8.4 HIGH
CVE-2026-58829	8.4 HIGH
CVE-2026-58836	7.8 HIGH
CVE-2026-58837	8.4 HIGH
CVE-2026-58838	4.0 MEDIUM
CVE-2026-58844	8.4 HIGH
CVE-2026-58845	8.4 HIGH
CVE-2026-58847	8.4 HIGH
CVE-2026-58853	7.5 HIGH

CVE	CVSS Score
CVE-2026-58857	
CVE-2026-58866	8.4 HIGH
CVE-2026-58867	8.4 HIGH
CVE-2026-58868	
CVE-2026-58870	
CVE-2026-58871	8.4 HIGH
CVE-2026-58875	6.2 MEDIUM
CVE-2026-58876	9.8 CRITICAL
CVE-2026-58877	4.0 MEDIUM
CVE-2026-58879	8.4 HIGH
CVE-2026-58882	
CVE-2026-58883	
CVE-2026-58884	8.4 HIGH
CVE-2026-58885	8.4 HIGH
CVE-2026-58886	
CVE-2026-58933	5.3 MEDIUM
CVE-2026-58934	8.4 HIGH
CVE-2026-58936	9.8 CRITICAL
CVE-2026-58937	6.2 MEDIUM
CVE-2026-58938	
CVE-2026-58942	8.4 HIGH
CVE-2026-58943	8.4 HIGH
CVE-2026-58944	8.4 HIGH
CVE-2026-58945	
CVE-2026-58946	8.4 HIGH
CVE-2026-58949	7.5 HIGH
CVE-2026-58951	
CVE-2026-58953	
CVE-2026-58955	6.2 MEDIUM
CVE-2026-58956	8.4 HIGH
CVE-2026-58957	8.4 HIGH

CVE	CVSS Score
CVE-2026-58958	
CVE-2026-58961	8.4 HIGH
CVE-2026-58962	8.4 HIGH
CVE-2026-58963	
CVE-2026-58964	8.4 HIGH
CVE-2026-58965	8.4 HIGH
CVE-2026-58966	8.4 HIGH
CVE-2026-58968	9.8 CRITICAL
CVE-2026-58969	
CVE-2026-58970	8.4 HIGH
CVE-2026-58971	
CVE-2026-58974	8.4 HIGH
CVE-2026-58975	8.4 HIGH
CVE-2026-58976	
CVE-2026-58977	6.7 MEDIUM
CVE-2026-58978	6.8 MEDIUM
CVE-2026-58979	8.4 HIGH
CVE-2026-58984	8.4 HIGH
CVE-2026-58985	6.2 MEDIUM
CVE-2026-58986	8.4 HIGH
CVE-2026-58988	4.0 MEDIUM
CVE-2026-58989	8.4 HIGH
CVE-2026-58990	
CVE-2026-58994	8.4 HIGH
CVE-2026-58995	8.4 HIGH
CVE-2026-58997	
CVE-2026-59000	8.4 HIGH
CVE-2026-59001	
CVE-2026-59002	
CVE-2026-59003	4.0 MEDIUM
CVE-2026-59004	8.4 HIGH

CVE	CVSS Score
CVE-2026-59005	8.4 HIGH
CVE-2026-59006	4.0 MEDIUM
CVE-2026-59007	5.3 MEDIUM
CVE-2026-59008	6.2 MEDIUM
CVE-2026-59010	6.2 MEDIUM
CVE-2026-59011	
CVE-2026-59012	
CVE-2026-59014	8.4 HIGH
CVE-2026-59015	4.0 MEDIUM
CVE-2026-59016	8.4 HIGH
CVE-2026-59020	5.9 MEDIUM
CVE-2026-59021	6.2 MEDIUM
CVE-2026-59022	
CVE-2026-59028	8.4 HIGH
CVE-2026-59031	6.2 MEDIUM
CVE-2026-59042	7.4 HIGH
CVE-2026-59043	7.4 HIGH
CVE-2026-59044	8.4 HIGH
CVE-2026-59045	7.4 HIGH
CVE-2026-59046	6.2 MEDIUM
CVE-2026-59047	6.2 MEDIUM
CVE-2026-59048	
CVE-2026-64011	7.8 HIGH
CVE-2026-64427	5.5 MEDIUM
CVE-2026-64560	7.8 HIGH
CVE-2026-65076	
CVE-2026-65586	
CVE-2026-65587	
CVE-2026-66086	9.8 CRITICAL
CVE-2026-66113	
CVE-2026-66114	

CVE	CVSS Score
CVE-2026-74912	
CVE-2026-79405	7.5 HIGH
CVE-2026-80013	
CVE-2026-80335	7.6 HIGH
CVE-2026-80336	
CVE-2026-80604	8.8 HIGH
CVE-2026-89774	8.8 HIGH

CWE's

CWE	Beschrijving
CWE-89	Improper Neutralization of Special Elements used in an SQL Command
CWE-22	Improper Limitation of a Pathname to a Restricted Directory
CWE-120	Buffer Copy without Checking Size of Input
CWE-121	Stack-based Buffer Overflow
CWE-122	Heap-based Buffer Overflow
CWE-123	Write-what-where Condition
CWE-125	Out-of-bounds Read
CWE-129	Improper Validation of Array Index
CWE-190	Integer Overflow or Wraparound
CWE-126	Buffer Over-read
CWE-248	Uncaught Exception
CWE-226	Sensitive Information in Resource Not Removed Before Reuse
CWE-617	Reachable Assertion
CWE-476	NULL Pointer Dereference
CWE-415	Double Free
CWE-416	Use After Free
CWE-347	Improper Verification of Cryptographic Signature
CWE-763	Release of Invalid Pointer or Reference

CWE	Beschrijving
CWE-653	Improper Isolation or Compartmentalization

Getroffen producten

Android
Android

Samsung
Android

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions:
NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.