



NCSC-2026-0173

Kwetsbaarheden verholpen in Google Android en Samsung Mobile

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 02-06-2026

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.

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

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.

Onder de verholpen kwetsbaarheden zit een aantal kwetsbaarheden die door Google worden gemarkeerd als 'Critical'.

Google heeft verder, zoals gebruikelijk, weinig detailinformatie beschikbaar gesteld.

Oplossingen

Google heeft updates uitgebracht om de kwetsbaarheden te verhelpen in Android 12,13 en 14.

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

Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://security.samsungmobile.com/securityUpdate.smsb?year=2026&month=6>
- <https://source.android.com/docs/security/bulletin/2026/2026-06-01>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-22424	8.5 HIGH
➤ CVE-2025-22426	8.5 HIGH
➤ CVE-2025-32348	8.5 HIGH
➤ CVE-2025-47384	6.5 MEDIUM

> CVE-2025-47392	8.8 HIGH
> CVE-2025-47400	7.1 HIGH
> CVE-2025-47401	6.5 MEDIUM
> CVE-2025-47403	6.5 MEDIUM
> CVE-2025-48570	8.5 HIGH
> CVE-2025-48595	8.4 HIGH
> CVE-2025-48615	7.8 HIGH
> CVE-2025-48649	8.5 HIGH
> CVE-2025-48652	8.5 HIGH
> CVE-2025-59604	7.8 HIGH
> CVE-2025-59605	7.8 HIGH
> CVE-2025-59606	7.8 HIGH
> CVE-2025-64505	5.3 MEDIUM
> CVE-2025-64720	5.3 MEDIUM
> CVE-2025-65018	5.3 MEDIUM
> CVE-2026-0009	8.5 HIGH
> CVE-2026-0016	3.3 LOW
> CVE-2026-0018	6.8 MEDIUM
> CVE-2026-0036	8.5 HIGH
> CVE-2026-0039	6.5 MEDIUM
> CVE-2026-0040	6.5 MEDIUM
> CVE-2026-0041	6.5 MEDIUM
> CVE-2026-0042	5.5 MEDIUM

> CVE-2026-0043	6.8 MEDIUM
> CVE-2026-0044	6.5 MEDIUM
> CVE-2026-0046	8.5 HIGH
> CVE-2026-0048	8.5 HIGH
> CVE-2026-0051	6.5 MEDIUM
> CVE-2026-0052	6.5 MEDIUM
> CVE-2026-0055	8.5 HIGH
> CVE-2026-0056	3.3 LOW
> CVE-2026-0059	8.6 HIGH
> CVE-2026-0061	4.8 MEDIUM
> CVE-2026-0069	6.8 MEDIUM
> CVE-2026-0070	6.8 MEDIUM
> CVE-2026-0076	4.8 MEDIUM
> CVE-2026-0077	8.5 HIGH
> CVE-2026-0078	8.5 HIGH
> CVE-2026-0080	7.1 HIGH
> CVE-2026-0087	8.5 HIGH
> CVE-2026-0089	8.5 HIGH
> CVE-2026-0091	8.5 HIGH
> CVE-2026-0097	8.6 HIGH
> CVE-2026-0100	8.5 HIGH
> CVE-2026-21017	
> CVE-2026-21025	

> CVE-2026-21026	
> CVE-2026-21027	
> CVE-2026-21028	
> CVE-2026-21029	
> CVE-2026-21030	
> CVE-2026-21031	
> CVE-2026-21352	7.8 HIGH
> CVE-2026-21353	7.8 HIGH
> CVE-2026-21367	7.6 HIGH
> CVE-2026-21372	7.8 HIGH
> CVE-2026-21373	7.8 HIGH
> CVE-2026-21374	7.8 HIGH
> CVE-2026-21375	7.8 HIGH
> CVE-2026-21376	7.8 HIGH
> CVE-2026-21378	7.8 HIGH
> CVE-2026-21380	7.8 HIGH
> CVE-2026-21381	7.6 HIGH
> CVE-2026-21547	
> CVE-2026-23787	
> CVE-2026-24085	7.2 HIGH
> CVE-2026-24089	7.2 HIGH
> CVE-2026-25276	8.8 HIGH
> CVE-2026-25277	8.8 HIGH

> CVE-2026-28577	5.3 MEDIUM
> CVE-2026-28578	6.8 MEDIUM
> CVE-2026-28580	8.5 HIGH
> CVE-2026-28586	4.8 MEDIUM

CWE's

CWE	Beschrijving
> CWE-20	Improper Input Validation
> 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-129	Improper Validation of Array Index
> CWE-190	Integer Overflow or Wraparound
> CWE-269	Improper Privilege Management
> CWE-400	Uncontrolled Resource Consumption
> CWE-416	Use After Free
> CWE-476	NULL Pointer Dereference
> CWE-617	Reachable Assertion
> CWE-693	Protection Mechanism Failure
> CWE-770	Allocation of Resources Without Limits or Throttling
> CWE-787	Out-of-bounds Write
> CWE-1021	Improper Restriction of Rendered UI Layers or Frames
> CWE-1286	Improper Validation of Syntactic Correctness of Input

Getroffen producten

Google
Android
Samsung
Mobile Devices

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.