



Advisory NCSC-2026-0405

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Google Android

Publicatiedatum: 07-10-2026

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 kwetsbaarheden betreffen onder andere onjuiste bounds checking, ontbrekende permissiecontroles, integer overflows, onjuist geïnitieerde pointers, type confusion, race conditions en onjuiste exception handling.

Deze fouten kunnen leiden tot out-of-bounds memory reads en writes, geheugen corruptie, privilege escalatie, informatielekken, denial-of-service situaties en controle over het systeem door een aanvaller. Exploitatie kan lokaal of op afstand plaatsvinden, vaak zonder dat er gebruikersinteractie of verhoogde rechten nodig zijn.

De kwetsbaarheden zijn aanwezig in diverse functies en modules die gebruikt worden in verschillende softwareomgevingen, waaronder Bluetooth subsystemen, netwerk parsing, device management en audio controllers.

Oplossingen

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

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>
- <https://source.android.com/docs/security/bulletin/2026/2026-10-01>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-21114	
CVE-2026-21115	
CVE-2026-21116	
CVE-2026-21117	
CVE-2026-21118	
CVE-2026-21119	
CVE-2026-21120	
CVE-2026-21121	
CVE-2026-21122	
CVE-2026-21123	
CVE-2026-21124	
CVE-2026-21125	
CVE-2026-21126	
CVE-2026-28667	5.5 MEDIUM
CVE-2026-45513	
CVE-2026-45516	
CVE-2026-45524	8.8 HIGH
CVE-2026-49878	7.2 HIGH
CVE-2026-49880	7.8 HIGH
CVE-2026-49885	7.8 HIGH
CVE-2026-49933	7.8 HIGH
CVE-2026-49937	7.8 HIGH
CVE-2026-55265	6.5 MEDIUM
CVE-2026-55266	7.8 HIGH
CVE-2026-55269	7.8 HIGH
CVE-2026-55270	7.8 HIGH
CVE-2026-55279	
CVE-2026-55280	8.8 HIGH
CVE-2026-55286	7.8 HIGH

CVE	CVSS Score
CVE-2026-58815	7.8 HIGH
CVE-2026-58834	5.5 MEDIUM
CVE-2026-58835	8.8 HIGH
CVE-2026-58841	7.8 HIGH
CVE-2026-58854	7.8 HIGH
CVE-2026-58856	3.3 LOW
CVE-2026-58859	7.8 HIGH
CVE-2026-58865	7.5 HIGH
CVE-2026-58880	7.0 HIGH

CWE's

CWE	Beschrijving
CWE-122	Heap-based Buffer Overflow
CWE-190	Integer Overflow or Wraparound
CWE-248	Uncaught Exception
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-441	Unintended Proxy or Intermediary ('Confused Deputy')
CWE-457	Use of Uninitialized Variable
CWE-787	Out-of-bounds Write
CWE-824	Access of Uninitialized Pointer
CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')
CWE-862	Missing Authorization

Getroffen producten

Google
Android

Samsung
Samsung Mobile

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 or 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.