



# NCSC-2026-0046

## Kwetsbaarheden verholpen in Samsung mobile

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 09-02-2026

**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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto:info@ncsc.nl)

## Feiten

Samsung heeft kwetsbaarheden verholpen in verschillende softwarecomponenten, waaronder Emergency Sharing, KnoxGuard Manager, Settings, PACM, FacAtFunction, ShortcutService en Samsung Dialer, specifiek voor de SMR Feb-2026 Release 1.

## Duiding

De kwetsbaarheden zijn gerelateerd aan onjuist toegangsbeheer, onjuiste autorisatie, onjuist privilegebeheer en onjuiste invoervalidatie. Deze kwetsbaarheden stellen lokale aanvallers in staat om ongeautoriseerde toegang te verkrijgen, systeeminstellingen te manipuleren, willekeurige commando's uit te voeren en bestanden met systeemprivileges te creëren. Dit kan leiden tot compromittering van de integriteit en vertrouwelijkheid van de getroffen systemen.

In deze update heeft Samsung ook oudere kwetsbaarheden in Google Android verholpen, welke relevant zijn voor Samsung Mobile.

Voor succesvol misbruik moet de kwaadwillende het slachtoffer misleiden een malafide app te downloaden en installeren, of een malafide link te volgen.

## Oplossingen

Samsung heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

## Referenties

➤ <https://security.samsungmobile.com/securityUpdate.smsb?year=2026&month=02>

## Kwetsbaarheden

CVE	CVSS Score
➤ <a href="#">CVE-2026-20977</a>	6.9 MEDIUM
➤ <a href="#">CVE-2026-20978</a>	5.8 MEDIUM
➤ <a href="#">CVE-2026-20979</a>	8.5 HIGH
➤ <a href="#">CVE-2026-20980</a>	7.0 HIGH

> CVE-2026-20981	5.4 MEDIUM
> CVE-2026-20982	6.8 MEDIUM
> CVE-2026-20983	8.4 HIGH

## CWE's

CWE	Beschrijving
> CVE-20	Improper Input Validation
> CVE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
> CVE-35	Path Traversal: '../../../'
> CVE-269	Improper Privilege Management
> CVE-284	Improper Access Control
> CVE-926	Improper Export of Android Application Components

## Getroffen producten

<b>Samsung</b>
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.