



# NCSC-2025-0072

## Kwetsbaarheden verholpen in Google Android en Samsung Mobile

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 04-03-2025

### **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](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

Google heeft meerdere kwetsbaarheden verholpen in Android en Samsung Mobile, waaronder twee zero-day kwetsbaarheden die actief werden uitgebuit in gerichte aanvallen.

## Duiding

De kwetsbaarheden bevinden zich in de Android-kernel en de ExternalStorageProvider.java, wat kan leiden tot lokale privilege-escalatie en remote code-executie. Daarnaast kunnen verschillende kwetsbaarheden remote aanvallers in staat stellen om denial-of-service te veroorzaken of gevoelige gegevens te benaderen. De kwetsbaarheden treffen verschillende versies van Android en Samsung-producten, wat onmiddellijke aandacht van beveiligingsbeheerders vereist.

Google meldt informatie te hebben ontvangen dat de kwetsbaarheden met kenmerk CVE-2024-43093 en CVE-2024-50302 beperkt en gericht zijn misbruikt. Deze kwetsbaarheden bevinden zich respectievelijk in het Android Framework en in de Kernel 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 heeft fixes geïmplementeerd om deze risico's te mitigeren, terwijl Samsung soortgelijke problemen in zijn apparaten heeft aangepakt. Zie bijgevoegde referenties voor meer informatie.

## Referenties

- <https://source.android.com/docs/security/bulletin/2025-03-01>
- <https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=03>

## Kwetsbaarheden

CVE	CVSS Score
➤ <a href="#">CVE-2023-21125</a>	
➤ <a href="#">CVE-2024-43051</a>	4.8 MEDIUM
➤ <a href="#">CVE-2024-43093</a>	7.8 HIGH
➤ <a href="#">CVE-2024-46852</a>	5.1 MEDIUM

> CVE-2024-49728	
> CVE-2024-49836	8.5 HIGH
> CVE-2024-49838	8.2 HIGH
> CVE-2024-50302	5.1 MEDIUM
> CVE-2024-53011	4.6 MEDIUM
> CVE-2024-53014	8.5 HIGH
> CVE-2024-53024	8.5 HIGH
> CVE-2024-53025	6.8 MEDIUM
> CVE-2024-53027	8.7 HIGH
> CVE-2025-0074	
> CVE-2025-0075	
> CVE-2025-0079	
> CVE-2025-0081	
> CVE-2025-0082	
> CVE-2025-0084	
> CVE-2025-0092	
> CVE-2025-0093	
> CVE-2025-20644	6.3 MEDIUM
> CVE-2025-20645	4.6 MEDIUM
> CVE-2025-20903	
> CVE-2025-20908	
> CVE-2025-20909	
> CVE-2025-20910	

<a href="#">&gt; CVE-2025-20911</a>
<a href="#">&gt; CVE-2025-20912</a>
<a href="#">&gt; CVE-2025-22403</a>
<a href="#">&gt; CVE-2025-22404</a>
<a href="#">&gt; CVE-2025-22405</a>
<a href="#">&gt; CVE-2025-22406</a>
<a href="#">&gt; CVE-2025-22407</a>
<a href="#">&gt; CVE-2025-22408</a>
<a href="#">&gt; CVE-2025-22409</a>
<a href="#">&gt; CVE-2025-22410</a>
<a href="#">&gt; CVE-2025-22411</a>
<a href="#">&gt; CVE-2025-22412</a>
<a href="#">&gt; CVE-2025-22413</a>
<a href="#">&gt; CVE-2025-26417</a>

## CWE's

CWE	Beschrijving
<a href="#">&gt; CVE-264</a>	CWE-264
<a href="#">&gt; CVE-126</a>	Buffer Over-read
<a href="#">&gt; CVE-193</a>	Off-by-one Error
<a href="#">&gt; CVE-1286</a>	Improper Validation of Syntactic Correctness of Input
<a href="#">&gt; CVE-908</a>	Use of Uninitialized Resource
<a href="#">&gt; CVE-129</a>	Improper Validation of Array Index
<a href="#">&gt; CVE-190</a>	Integer Overflow or Wraparound

➤ <a href="#">CWE-665</a>	Improper Initialization
➤ <a href="#">CWE-285</a>	Improper Authorization
➤ <a href="#">CWE-476</a>	NULL Pointer Dereference
➤ <a href="#">CWE-787</a>	Out-of-bounds Write
➤ <a href="#">CWE-200</a>	Exposure of Sensitive Information to an Unauthorized Actor
➤ <a href="#">CWE-120</a>	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

## Getroffen producten

<b>Android</b>
System
<b>Samsung</b>
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.