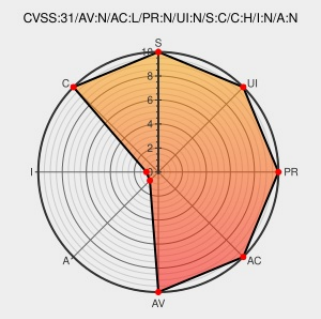
CVE-2021-25374

Published on: 04/09/2021 12:00:00 AM UTC

Last Modified on: 07/14/2022 03:44:00 PM UTC

CVE-2021-25374

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Android from Google contain the following vulnerability:

An improper authorization vulnerability in Samsung Members "samsungrewards" scheme for deeplink in versions 2.4.83.9 in Android O(8.1) and below, and 3.9.00.9 in Android P(9.0) and above allows remote attackers to access a user data related with Samsung Account.

CVE-2021-25374 has been assigned by mobile.security@samsung.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Samsung Mobile** - **Samsung Members** version **< 2.4.83.9**

Affected Vendor/Software: **Samsung Mobile** - **Samsung Members** version **< 3.9.00.9**

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link

Samsung Mobile Security	security.samsungmobile.com text/html	CONFIRM security.samsungmobile.com/serviceWeb.smsb
No Description Provided	security.samsungmobile.com text/html	CONFIRM security.samsungmobile.com/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

This script can be used to gain access to a victim's Samsung Account if they have a specific version of Samsung Membe…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	8.1	All	All	All
Operating System	Google	Android	9.0	All	All	All
Application	Samsung	Members	All	All	All	All
Application	Samsung	Members	All	All	All	All

cpe:2.3:o:google:android:8.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:9.0:*:*:*:*:*:*:*:

cpe:2.3:a:samsung:members:*:*:*:*:*:*:*:*:

cpe:2.3:a:samsung:members:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-25374 : An improper authorization vulnerability in Samsung Members "samsungrewards" scheme for deeplink in… twitter.com/i/web/status/1…	2021-04-09 18:14:15
@SecRiskRptSME	RT: CVE-2021-25374 An improper authorization vulnerability in Samsung Members "samsungrewards" scheme for deeplink… twitter.com/i/web/status/1…	2021-04-11 07:36:21
@AlirezaGhahrood	exploit CVE-2021-25374: An improper authorization vulnerability in Samsung Members "samsungrewards" scheme for deep… twitter.com/i/web/status/1…	2021-04-11 19:30:39
@nuria_imeq	GitHub - FSecureLABS/CVE-2021-25374_Samsung-Account-Access github.com/FSecureLABS/CV…	2021-04-11 19:34:39

@keithyperss	CVE-2021-25374 : Samsung Account Access Script github.com/FSecureLABS/CV…	2021-05-02 08:50:14
@RemotelyAlerts	Severity: ?? | An improper authorization vulnerability ... | CVE-2021-25374 | Link for more: alerts.remotelyrmm.com/CVE-2021-25374	2022-07-14 17:32:10
/r/netcve	CVE-2021-25374	2021-04-09 18:28:12

← Previous ID

Next ID→