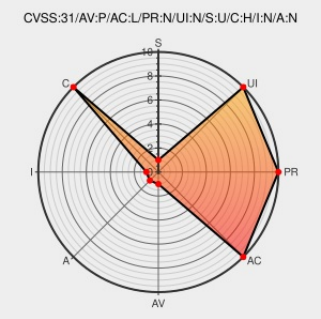
CVE-2019-11341

Published on: 10/09/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:35 PM UTC

CVE-2019-11341

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



Certain versions of Android from Google contain the following vulnerability:

On certain Samsung P(9.0) phones, an attacker with physical access can start a TCP Dump capture without the user's knowledge. This feature of the Service Mode application is available after entering the *#9900# check code, but is protected by an OTP password. However, this password is created locally and (due to mishandling of cryptography) can be obtained easily by reversing the password creation logic.

CVE-2019-11341 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 4.6 - MEDIUM

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

CVSS2 Score: 2.1 - LOW

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

CVE References

Description	Tags	Link
Most Complete Samsung Galaxy Secret Code List!- Dr.Fone	Third Party Advisory drfone.wondershare.com	MISC drfone.wondershare.com/unlock/samsung-galaxy-

	text/html	secret-code-list.html
Elliot Alderson on Twitter: "THREAD: If you have a @SamsungMobile phones, whatever your phone model, an attacker with a physical access to your phone can capture your network traffic without your consent. Let me show you ⬇⬇⬇… https://t.co/uRHFj6EnVR"	Exploit Third Party Advisory nitter.domain.glass text/html	MISC twitter.com/fs0c131y/status/1115889065285562368
Samsung Mobile Security	Not Applicable security.samsungmobile.com text/html	MISC security.samsungmobile.com/securityUpdate.smsb

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

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	9.0	All	All	All
Operating System	Google	Android	9.0	All	All	All
Hardware	Samsung	Phone	-	All	All	All
Hardware	Samsung	Phone	-	All	All	All

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

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

cpe:2.3:h:samsung:phone:-:*:*:*:*:*:*:*:

cpe:2.3:h:samsung:phone:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→