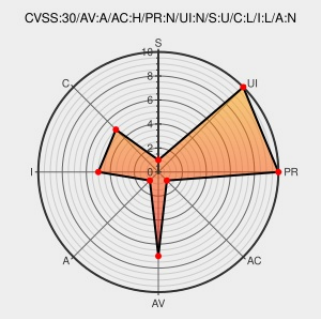
CVE-2019-5307

Published on: 06/04/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:00 PM UTC

CVE-2019-5307

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



Certain versions of P30 from Huawei contain the following vulnerability:

Some Huawei 4G LTE devices, P30 versions before ELE-AL00 9.1.0.162(C01E160R1P12/C01E160R2P1) and P30 Pro versions before VOG-AL00 9.1.0.162(C01E160R1P12/C01E160R2P1), are exposed to a message replay vulnerability. For the sake of better compatibility, these devices implement a less strict check on the NAS message sequence number (SN), specifically NAS COUNT. As a result, an attacker can construct a rogue base station and replay the GUTI reallocation command message in certain conditions to tamper with GUTIs, or replay the Identity request message to obtain IMSIs. (Vulnerability ID: HWPSIRT-2019-04107)

CVE-2019-5307 has been assigned by psirt@huawei.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Huawei** - **P30,P30 Pro** version **The versions before ELE-AL00 9.1.0.162(C01E160R1P12/C01E160R2P1)**

Affected Vendor/Software: **Huawei** - **P30,P30 Pro** version **The versions before VOG-AL00 9.1.0.162(C01E160R1P12/C01E160R2P1)**

CVSS3 Score: 4.2 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
Security Advisory - Some Huawei 4G LTE devices are exposed to a message replay vulnerability	Vendor Advisory www.huawei.com text/html	CONFIRM www.huawei.com/en/psirt/security-advisories/huawei-sa-20190529-01-replay-en

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Huawei	P30	-	All	All	All
Hardware	Huawei	P30	-	All	All	All
Operating System	Huawei	P30 Firmware	All	All	All	All
Operating System	Huawei	P30 Firmware	All	All	All	All
Hardware	Huawei	P30 Pro	-	All	All	All
Hardware	Huawei	P30 Pro	-	All	All	All
Operating System	Huawei	P30 Pro Firmware	All	All	All	All
Operating System	Huawei	P30 Pro Firmware	All	All	All	All

cpe:2.3:h:huawei:p30:-:*:*:*:*:*:*:*:

cpe:2.3:h:huawei:p30:-:*:*:*:*:*:*:*:

cpe:2.3:o:huawei:p30_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:huawei:p30_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:huawei:p30_pro:-:*:*:*:*:*:*:*:

cpe:2.3:h:huawei:p30_pro:-:*:*:*:*:*:*:*:

cpe:2.3:o:huawei:p30_pro_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:huawei:p30_pro_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→