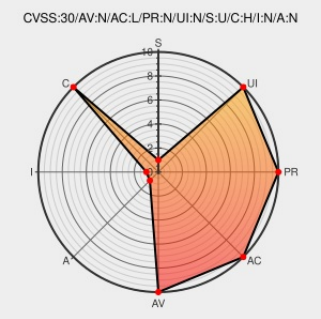
CVE-2017-8174

Published on: 11/22/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:42 PM UTC

CVE-2017-8174

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



Certain versions of Secospace Usg6300 from Huawei contain the following vulnerability:

Huawei USG6300 V100R001C30SPC300 and USG6600 with software of V100R001C30SPC500,V100R001C30SPC600,V100R001C30SPC700,V100R001C30SPC800 have a weak algorithm vulnerability. Attackers may exploit the weak algorithm vulnerability to crack the cipher text and cause confidential information leaks on the transmission links.

CVE-2017-8174 has been assigned by psirt@huawei.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Huawei Technologies Co., Ltd.** - **Secospace USG6300,Secospace USG6600** version **V100R001C30SPC300,V100R001C30SPC500,V100R001C30SPC600,V100R001C30SPC700,V100R001C30SPC800**

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
Security Advisory - Weak Algorithm Vulnerability in Huawei USG product	Vendor Advisory www.huawei.com text/html	CONFIRM www.huawei.com/en/psirt/security-advisories/huawei-sa-20170802-01-usg-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	Secospace Usg6300	-	All	All	All
Hardware	Huawei	Secospace Usg6300	-	All	All	All
Operating System	Huawei	Secospace Usg6300 Firmware	v100r001c30spc300	All	All	All
Operating System	Huawei	Secospace Usg6300 Firmware	v100r001c30spc300	All	All	All
Hardware	Huawei	Secospace Usg6600	-	All	All	All
Hardware	Huawei	Secospace Usg6600	-	All	All	All
Operating System	Huawei	Secospace Usg6600 Firmware	v100r001c30spc500	All	All	All
Operating System	Huawei	Secospace Usg6600 Firmware	v100r001c30spc600	All	All	All
Operating System	Huawei	Secospace Usg6600 Firmware	v100r001c30spc700	All	All	All
Operating System	Huawei	Secospace Usg6600 Firmware	v100r001c30spc800	All	All	All
Operating System	Huawei	Secospace Usg6600 Firmware	v100r001c30spc500	All	All	All
Operating System	Huawei	Secospace Usg6600 Firmware	v100r001c30spc600	All	All	All
Operating System	Huawei	Secospace Usg6600 Firmware	v100r001c30spc700	All	All	All
Operating System	Huawei	Secospace Usg6600 Firmware	v100r001c30spc800	All	All	All

cpe:2.3:h:huawei:secospace_usg6300:-:*:*:*:*:*:*:*:

cpe:2.3:h:huawei:secospace_usg6300:-:*:*:*:*:*:*:*:

cpe:2.3:o:huawei:secospace_usg6300_firmware:v100r001c30spc300:*:*:*:*:*:*:*:

cpe:2.3:o:huawei:secospace_usg6300_firmware:v100r001c30spc300:*:*:*:*:*:*:*:

cpe:2.3:h:huawei:secospace_usg6600:-:*:*:*:*:*:*:*:

cpe:2.3:h:huawei:secospace_usg6600:-:*:*:*:*:*:*:*:

cpe:2.3:o:huawei:secospace_usg6600_firmware:v100r001c30spc500:*:*:*:*:*:*:*:

cpe:2.3:o:huawei:secospace_usg6600_firmware:v100r001c30spc600:*:*:*:*:*:*:*:

cpe:2.3:o:huawei:secospace_usg6600_firmware:v100r001c30spc700:*:*:*:*:*:*:*:

cpe:2.3:o:huawei:secospace_usg6600_firmware:v100r001c30spc800:*:*:*:*:*:*:*:

cpe:2.3:o:huawei:secospace_usg6600_firmware:v100r001c30spc500:*:*:*:*:*:*:*:

cpe:2.3:o:huawei:secospace_usg6600_firmware:v100r001c30spc600:*:*:*:*:*:*:*:

cpe:2.3:o:huawei:secospace_usg6600_firmware:v100r001c30spc700:*:*:*:*:*:*:*:

cpe:2.3:o:huawei:secospace_usg6600_firmware:v100r001c30spc800:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→