

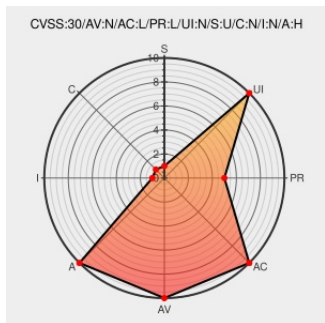


CVE-2017-15315

Published on: 03/09/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:32 PM UTC

CVE-2017-15315

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Nip6300](#) from [Huawei](#) contain the following vulnerability:

Patch module of Huawei NIP6300 V500R001C20SPC100, V500R001C20SPC200, NIP6600 V500R001C20SPC100, V500R001C20SPC200, Secospace USG6300 V500R001C20SPC100, V500R001C20SPC200, Secospace USG6500 V500R001C20SPC100, V500R001C20SPC200 has a memory leak vulnerability. An

authenticated attacker could execute special commands many times, the memory leaking happened, which would cause the device to reset finally.

CVE-2017-15315 has been assigned by psirt@huawei.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: Huawei Technologies Co., Ltd. - NIP6300, NIP6600, Secospace USG6300, Secospace USG6500 version NIP6300 V500R001C20SPC100, V500R001C20SPC200, NIP6600 V500R001C20SPC100, V500R001C20SPC200, Secospace USG6300 V500R001C20SPC100, V500R001C20SPC200, Secospace USG6500 V500R001C20SPC100, V500R001C20SPC200

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	COMPLETE

CVE References

Description

Tags

Link

Security Advisory - Memory Leak Vulnerability in Some Huawei Network Products

Vendor Advisory

www.huawei.com

text/html



CONFIRM www.huawei.com/en/psirt/security-advisories/huawei-sa-20171129-01-command-en

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
Hardware	Huawei	Nip6300	-	All	All	All
Hardware	Huawei	Nip6300	-	All	All	All
Operating System	Huawei	Nip6300 Firmware	v500r001c20spc100	All	All	All
Operating System	Huawei	Nip6300 Firmware	v500r001c20spc200	All	All	All
Operating System	Huawei	Nip6300 Firmware	v500r001c20spc100	All	All	All
Operating System	Huawei	Nip6300 Firmware	v500r001c20spc200	All	All	All
Hardware	Huawei	Nip6600	-	All	All	All
Hardware	Huawei	Nip6600	-	All	All	All
Operating System	Huawei	Nip6600 Firmware	v500r001c20spc100	All	All	All
Operating System	Huawei	Nip6600 Firmware	v500r001c20spc200	All	All	All
Operating System	Huawei	Nip6600 Firmware	v500r001c20spc100	All	All	All
Operating System	Huawei	Nip6600 Firmware	v500r001c20spc200	All	All	All
Hardware	Huawei	Secospace Usg6300	-	All	All	All
Hardware	Huawei	Secospace Usg6300	-	All	All	All
Operating System	Huawei	Secospace Usg6300 Firmware	v500r001c20spc100	All	All	All
Operating System	Huawei	Secospace Usg6300 Firmware	v500r001c20spc200	All	All	All
Operating System	Huawei	Secospace Usg6300 Firmware	v500r001c20spc100	All	All	All

Operating System	Huawei	Secospace Usg6300 Firmware	v500r001c20spc200	All	All	All
Hardware 	Huawei	Secospace Usg6500	-	All	All	All
Hardware 	Huawei	Secospace Usg6500	-	All	All	All
Operating System	Huawei	Secospace Usg6500 Firmware	v500r001c20spc100	All	All	All
Operating System	Huawei	Secospace Usg6500 Firmware	v500r001c20spc200	All	All	All
Operating System	Huawei	Secospace Usg6500 Firmware	v500r001c20spc100	All	All	All
Operating System	Huawei	Secospace Usg6500 Firmware	v500r001c20spc200	All	All	All
cpe:2.3:h:huawei:nip6300:-:*:*:*:*:*:						
cpe:2.3:h:huawei:nip6300:-:*:*:*:*:*:						
cpe:2.3:o:huawei:nip6300_firmware:v500r001c20spc100:*:*:*:*:*:						
cpe:2.3:o:huawei:nip6300_firmware:v500r001c20spc200:*:*:*:*:*:						
cpe:2.3:o:huawei:nip6300_firmware:v500r001c20spc100:*:*:*:*:*:						
cpe:2.3:o:huawei:nip6300_firmware:v500r001c20spc200:*:*:*:*::~						
cpe:2.3:h:huawei:nip6600:-:*:*:*:*:*:						
cpe:2.3:h:huawei:nip6600:-:*:*:*:*::~						
cpe:2.3:o:huawei:nip6600_firmware:v500r001c20spc100:*:*:*:*::~						
cpe:2.3:o:huawei:nip6600_firmware:v500r001c20spc200:*:*:*:*::~						
cpe:2.3:o:huawei:nip6600_firmware:v500r001c20spc100:*:*:*:*::~						
cpe:2.3:o:huawei:nip6600_firmware:v500r001c20spc200:*:*:*:*::~						
cpe:2.3:h:huawei:secospace_usg6300:-:*:*:*:*::~						
cpe:2.3:h:huawei:secospace_usg6300:-:*:*:*:*::~						
cpe:2.3:o:huawei:secospace_usg6300_firmware:v500r001c20spc100:*:*:*:*::~						
cpe:2.3:o:huawei:secospace_usg6300_firmware:v500r001c20spc200:*:*:*:*::~						
cpe:2.3:o:huawei:secospace_usg6300_firmware:v500r001c20spc100:*:*:*:*::~						
cpe:2.3:o:huawei:secospace_usg6300_firmware:v500r001c20spc200:*:*:*:*::~						
cpe:2.3:h:huawei:secospace_usg6500:-:*:*:*:*::~						
cpe:2.3:h:huawei:secospace_usg6500:-:*:*:*:*::~						

```
cpe:2.3:o:huawei:secospace_usg6500_firmware:v500r001c20spc100:*.***.***.***
```

```
cpe:2.3:o:huawei:secospace_usg6500_firmware:v500r001c20spc200:*.***.***.
```

```
cpe:2.3:o:huawei:secospace_usg6500_firmware:v500r001c20spc100:*.***.*.***.*.
```

```
cpe:2.3:o:huawei:secospace_usg6500_firmware:v500r001c20spc200:*.~::~:~::~:
```

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report