



CVE-2018-7994

Published on: 07/31/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:37 PM UTC

CVE-2018-7994

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

CVSS:30/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H



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

Some Huawei products IPS Module V500R001C50; NGFW Module V500R001C50; V500R002C10; NIP6300 V500R001C50; NIP6600 V500R001C50; NIP6800 V500R001C50; Secospace USG6600 V500R001C50; USG9500 V500R001C50 have a memory leak

vulnerability. The software does not release allocated memory properly when processing Protal questionnaire. A remote attacker could send a lot questionnaires to the device, successful exploit could cause the device to reboot since running out of memory.

CVE-2018-7994 has been assigned by psirt@huawei.com to track the vulnerability - currently rated as **HIGH** severity.

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	NONE	NONE	HIGH

CVSS2 Score: **7.8 - HIGH**

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

CVE References

Description	Tags	Link
Security Advisory: Memory Leak Vulnerability on	Vulnerability	CONFIRM www.huawei.com/en/psirt/security

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	Ips Module	-	All	All	All
Hardware 	Huawei	Ips Module	-	All	All	All
Operating System	Huawei	Ips Module	v500r001c50	All	All	All
Operating System	Huawei	Ips Module	v500r001c50	All	All	All
Hardware 	Huawei	Ngfw Module	-	All	All	All
Hardware 	Huawei	Ngfw Module	-	All	All	All
Operating System	Huawei	Ngfw Module	v500r001c50	All	All	All
Operating System	Huawei	Ngfw Module	v500r002c10	All	All	All
Operating System	Huawei	Ngfw Module	v500r001c50	All	All	All
Operating System	Huawei	Ngfw Module	v500r002c10	All	All	All
Hardware 	Huawei	Nip6300	-	All	All	All
Hardware 	Huawei	Nip6300	-	All	All	All
Operating System	Huawei	Nip6300	v500r001c50	All	All	All
Operating System	Huawei	Nip6300	v500r001c50	All	All	All
Hardware 	Huawei	Nip6600	-	All	All	All
Hardware 	Huawei	Nip6600	-	All	All	All
Operating System	Huawei	Nip6600	v500r001c50	All	All	All
Operating System	Huawei	Nip6600	v500r001c50	All	All	All
Hardware 	Huawei	Nip6800	-	All	All	All

Hardware		Huawei	Nip6800	-	All	All	All
Operating System		Huawei	Nip6800	v500r001c50	All	All	All
Operating System		Huawei	Nip6800	v500r001c50	All	All	All
Hardware		Huawei	Secospace Usg6600	-	All	All	All
Hardware		Huawei	Secospace Usg6600	-	All	All	All
Operating System		Huawei	Secospace Usg6600	v500r001c50	All	All	All
Operating System		Huawei	Secospace Usg6600	v500r001c50	All	All	All
Hardware		Huawei	Usg9500	-	All	All	All
Hardware		Huawei	Usg9500	-	All	All	All
Operating System		Huawei	Usg9500	v500r001c50	All	All	All
Operating System		Huawei	Usg9500	v500r001c50	All	All	All
cpe:2.3:h:huawei:ips_module:-:*~::~:							
cpe:2.3:h:huawei:ips_module:-:*~::~:							
cpe:2.3:o:huawei:ips_module:v500r001c50:*~::~:							
cpe:2.3:o:huawei:ips_module:v500r001c50:*~::~:							
cpe:2.3:h:huawei:ngfw_module:-:*~::~:							
cpe:2.3:h:huawei:ngfw_module:-:*~::~:							
cpe:2.3:o:huawei:ngfw_module:v500r001c50:*~::~:							
cpe:2.3:o:huawei:ngfw_module:v500r002c10:*~::~:							
cpe:2.3:o:huawei:ngfw_module:v500r001c50:*~::~:							
cpe:2.3:o:huawei:ngfw_module:v500r002c10:*~::~:							
cpe:2.3:h:huawei:nip6300:-:*~::~:							
cpe:2.3:h:huawei:nip6300:-:*~::~:							
cpe:2.3:o:huawei:nip6300:v500r001c50:*~::~:							
cpe:2.3:o:huawei:nip6300:v500r001c50:*~::~:							
cpe:2.3:h:huawei:nip6600:-:*~::~:							
cpe:2.3:h:huawei:nip6600:-:*~::~:							
cpe:2.3:o:huawei:nip6600:v500r001c50:*~::~:							

cpe:2.3:o:huawei:nip6600:v500r001c50:*~::~:
cpe:2.3:h:huawei:nip6800:-~::~:
cpe:2.3:h:huawei:nip6800:-~::~:
cpe:2.3:o:huawei:nip6800:v500r001c50:*~::~:
cpe:2.3:o:huawei:nip6800:v500r001c50:*~::~:
cpe:2.3:h:huawei:secospace_usg6600:-~::~:
cpe:2.3:h:huawei:secospace_usg6600:-~::~:
cpe:2.3:o:huawei:secospace_usg6600:v500r001c50:*~::~:
cpe:2.3:o:huawei:secospace_usg6600:v500r001c50:*~::~:
cpe:2.3:h:huawei:usg9500:-~::~:
cpe:2.3:h:huawei:usg9500:-~::~:
cpe:2.3:o:huawei:usg9500:v500r001c50:*~::~:
cpe:2.3:o:huawei:usg9500:v500r001c50:*~::~:

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