

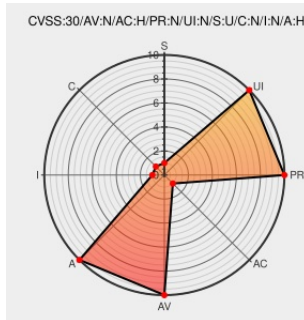


CVE-2017-17216

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

Last Modified on: 03/23/2021 11:26:27 PM UTC

CVE-2017-17216

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

Certain versions of [Dp300](#) from [Huawei](#) contain the following vulnerability:

Media Gateway Control Protocol (MGCP) in Huawei DP300 V500R002C00; RP200 V500R002C00SPC200; V600R006C00; TE30 V100R001C10; V500R002C00; V600R006C00; TE40 V500R002C00; V600R006C00; TE50 V500R002C00; V600R006C00; TE60 V100R001C10; V500R002C00; V600R006C00 have an out-of-bounds read vulnerability. An unauthenticated, remote attacker crafts malformed packets with specific parameter to the affected products. Due to insufficient validation of packets, successful exploitation may cause process reboot.

CVE-2017-17216 has been assigned by psirt@huawei.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.9 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
-------------	------	------

Security Advisory - Two Vulnerabilities in MGCP Protocol of Some Huawei Products

Vendor Advisory

www.huawei.com

text/html



CONFIRM www.huawei.com/en/psirt/security-advisories/huawei-sa-20180124-01-mgcp-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	Dp300	-	All	All	All
Hardware  	Huawei	Dp300	-	All	All	All
Operating System	Huawei	Dp300 Firmware	v500r002c00	All	All	All
Operating System	Huawei	Dp300 Firmware	v500r002c00	All	All	All
Hardware  	Huawei	Rp200	-	All	All	All
Hardware  	Huawei	Rp200	-	All	All	All
Operating System	Huawei	Rp200 Firmware	v500r002c00spc200	All	All	All
Operating System	Huawei	Rp200 Firmware	v600r006c00	All	All	All
Operating System	Huawei	Rp200 Firmware	v500r002c00spc200	All	All	All
Operating System	Huawei	Rp200 Firmware	v600r006c00	All	All	All
Hardware  	Huawei	Te30	-	All	All	All
Hardware  	Huawei	Te30	-	All	All	All
Operating System	Huawei	Te30 Firmware	v100r001c10	All	All	All
Operating System	Huawei	Te30 Firmware	v500r002c00	All	All	All
Operating System	Huawei	Te30 Firmware	v600r006c00	All	All	All
Operating System	Huawei	Te30 Firmware	v100r001c10	All	All	All
Operating System	Huawei	Te30 Firmware	v500r002c00	All	All	All
Operating System	Huawei	Te30 Firmware	v600r006c00	All	All	All

cpe:2.3:h:huawei:rp200:-:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:huawei:rp200_firmware:v500r002c00spc200:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:huawei:rp200_firmware:v600r006c00:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:huawei:rp200_firmware:v500r002c00spc200:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:huawei:rp200_firmware:v600r006c00:~::~~::~~::~~::~~::~~:::
cpe:2.3:h:huawei:te30:-:~::~~::~~::~~::~~::~~:::
cpe:2.3:h:huawei:te30:-:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:huawei:te30_firmware:v100r001c10:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:huawei:te30_firmware:v500r002c00:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:huawei:te30_firmware:v600r006c00:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:huawei:te30_firmware:v100r001c10:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:huawei:te30_firmware:v500r002c00:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:huawei:te30_firmware:v600r006c00:~::~~::~~::~~::~~::~~:::
cpe:2.3:h:huawei:te40:-:~::~~::~~::~~::~~::~~:::
cpe:2.3:h:huawei:te40:-:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:huawei:te40_firmware:v500r002c00:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:huawei:te40_firmware:v600r006c00:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:huawei:te40_firmware:v500r002c00:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:huawei:te40_firmware:v600r006c00:~::~~::~~::~~::~~::~~:::
cpe:2.3:h:huawei:te50:-:~::~~::~~::~~::~~::~~:::
cpe:2.3:h:huawei:te50:-:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:huawei:te50_firmware:v500r002c00:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:huawei:te50_firmware:v600r006c00:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:huawei:te50_firmware:v500r002c00:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:huawei:te50_firmware:v600r006c00:~::~~::~~::~~::~~::~~:::
cpe:2.3:h:huawei:te60:-:~::~~::~~::~~::~~::~~:::
cpe:2.3:h:huawei:te60:-:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:huawei:te60_firmware:v100r001c10:~::~~::~~::~~::~~::~~:::
cpe:2.3:o:huawei:te60_firmware:v500r002c00:~::~~::~~::~~::~~::~~:::

cpe:2.3:o:huawei:te60_firmware:v600r006c00:*****:
cpe:2.3:o:huawei:te60_firmware:v100r001c10:*****:
cpe:2.3:o:huawei:te60_firmware:v500r002c00:*****:
cpe:2.3:o:huawei:te60_firmware:v600r006c00:*****:

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](#)