



CVE-2017-11580

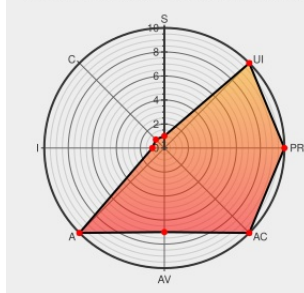
Published on: 07/02/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:25 PM UTC

CVE-2017-11580

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

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



Certain versions of [Wi-fi Blood Pressure Monitor](#) from [Blipcare](#) contain the following vulnerability:

Blipcare Wifi blood pressure monitor BP700 10.1 devices allow memory corruption that results in Denial of Service. When connected to the "Blip" open wireless connection provided by the device, if a large string is sent as a part of the HTTP request in any part of the HTTP headers, the device could become completely unresponsive.

Presumably this happens as the memory footprint provided to this device is very small. According to the specs from Rezolt, the Wi-Fi module only has 256k of memory. As a result, an incorrect string copy operation using either memcpy, strcpy, or any of their other variants could result in filling up the memory space allocated to the function executing and this would result in memory corruption. To test the theory, one can modify the demo application provided by the Cypress WICED SDK and introduce an incorrect "memcpy" operation and use the compiled application on the evaluation board provided by Cypress semiconductors with exactly the same Wi-Fi SOC. The results were identical where the device would completely stop responding to any of the ping or web requests.

CVE-2017-11580 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **6.1 - MEDIUM**

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	NONE

Confidentiality Impact

NONE

Integrity Impact

NONE

Availability Impact

COMPLETE

CVE References

Description	Tags	Link
Blipcare Clear Text Communication / Memory Corruption ~ Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/153225/Blipcare-Clear-Text-Communication-Memory-Corruption.html
IoT_vulnerabilities/Blipcare_sec_issues.pdf at master · ethanhunnt/IoT_vulnerabilities · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/ethanhunnt/IoT_vulnerabilities/blob/master/Blipcare_sec_issues.pdf
Bugtraq: Newly releases IoT security issues	Mailing List Third Party Advisory seclists.org text/html	BUGTRAQ 20190609 Newly releases IoT security issues

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	Blipcare	Wi-fi Blood Pressure Monitor	-	All	All	All
Hardware	Blipcare	Wi-fi Blood Pressure Monitor	-	All	All	All
Operating System	Blipcare	Wi-fi Blood Pressure Monitor Firmware	All	All	All	All

cpe:2.3:h:blipcare:wi-fi_blood_pressure_monitor:-:*:*:*:*:*:*:

cpe:2.3:h:blipcare:wi-fi_blood_pressure_monitor:-:*:*:*:*:*:*:

cpe:2.3:o:blipcare:wi-fi_blood_pressure_monitor_firmware:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →

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](#)