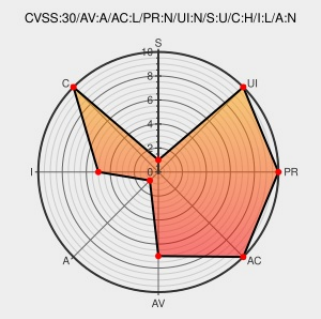
CVE-2017-11579

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

Last Modified on: 03/23/2021 11:26:24 PM UTC

CVE-2017-11579

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



Certain versions of Wi-fi Blood Pressure Monitor from Blipcare contain the following vulnerability:

In the most recent firmware for Blipcare, the device provides an open Wireless network called "Blip" for communicating with the device. The user connects to this open Wireless network and uses the web management interface of the device to provide the user's Wi-Fi credentials so that the device can connect to it and have Internet access. This device acts as a Wireless Blood pressure monitor and is used to measure blood pressure levels of a person. This allows an attacker who is in vicinity of Wireless signal generated by the Blipcare device to easily sniff the credentials. Also, an attacker can connect to the open wireless network "Blip" exposed by the device and modify the HTTP response presented to the user by the device to execute other attacks such as convincing the user to download and execute a malicious binary that would infect a user's computer or mobile device with malware.

CVE-2017-11579 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.1 - HIGH

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

CVSS2 Score: 4.8 - MEDIUM

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

PARTIAL | PARTIAL | NONE

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_i
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→

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