



CVE-2019-12941

Published on: 10/14/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:41 PM UTC

CVE-2019-12941

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

Certain versions of [4g/lte](#) from [Autopi](#) contain the following vulnerability:

AutoPi Wi-Fi/NB and 4G/LTE devices before 2019-10-15 allows an attacker to perform a brute-force attack or dictionary attack to gain access to the WiFi network, which provides root access to the device. The default WiFi password and WiFi SSID are derived from the same hash function output (input is only 8 characters), which allows an attacker to deduce the WiFi password from the WiFi SSID.

CVE-2019-12941 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **10 - HIGH**

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

CVE References

Description	Tags	Link
	Exploit Third Party Advisory	★ MISC www.diva-portal.org/smash/get/diva2:1334244/FULLTEXT01.pdf

www.diva-portal.org
[application/pdf](#)

[Exploit](#)
[Third Party Advisory](#)
www.kth.se
[application/pdf](#)

 MISC

www.kth.se/polopoly_fs/1.931922.1571071632!/Burdzovic_Matsson_dongle_v2.pdf

Software Systems Architecture
and Security | KTH

[Third Party Advisory](#)
www.kth.se
[text/html](#)

 MISC

www.kth.se/nse/research/software-systems-architecture-and-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 	Autopi	4g/lte	-	All	All	All
Operating System	Autopi	4g/lte Firmware	All	All	All	All
Hardware 	Autopi	4g/lte	-	All	All	All
Hardware 	Autopi	4g/lte	-	All	All	All
Operating System	Autopi	4g/lte Firmware	All	All	All	All
Operating System	Autopi	4g/lte Firmware	All	All	All	All
Hardware 	Autopi	Wi-fi/nb	-	All	All	All
Operating System	Autopi	Wi-fi/nb Firmware	All	All	All	All
Hardware 	Autopi	Wi-fi/nb	-	All	All	All
Hardware 	Autopi	Wi-fi/nb	-	All	All	All
Operating System	Autopi	Wi-fi/nb Firmware	All	All	All	All
Operating System	Autopi	Wi-fi/nb Firmware	All	All	All	All

cpe:2.3:h:autopi:4g/lte:-:~::~~::~~::~~::~~::~~::~~:::

cpe:2.3:o:autopi:4g/lte_firmware:~::~~::~~::~~::~~::~~::~~:::

cpe:2.3:h:autopi:4g/lte:-:~::~~::~~::~~::~~::~~::~~:::

cpe:2.3:h:autopi:4g/lte:-:~::~~::~~::~~::~~::~~::~~:::

cpe:2.3:o:autopi:4g\lte_firmware:~::~::~:
cpe:2.3:o:autopi:4g\lte_firmware:~::~::~:
cpe:2.3:h:autopi:wi-fi\nb:~::~::~:
cpe:2.3:o:autopi:wi-fi\nb_firmware:~::~::~:
cpe:2.3:h:autopi:wi-fi\nb:~::~::~:
cpe:2.3:h:autopi:wi-fi\nb:~::~::~:
cpe:2.3:o:autopi:wi-fi\nb_firmware:~::~::~:
cpe:2.3:o:autopi:wi-fi\nb_firmware:~::~::~:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)