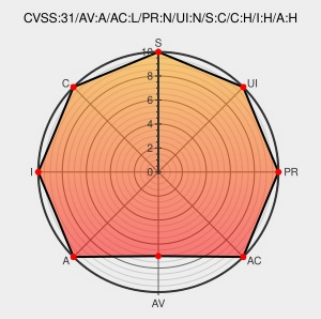
CVE-2020-8105

Published on: 12/20/2021 12:00:00 AM UTC

Last Modified on: 01/03/2022 06:09:00 PM UTC

CVE-2020-8105

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



Certain versions of Iota All-in-one Security Kit from Goabode contain the following vulnerability:

OS Command Injection vulnerability in the wirelessConnect handler of Abode iota All-In-One Security Kit allows an attacker to inject commands and gain root access. This issue affects: Abode iota All-In-One Security Kit versions prior to 1.0.2.23_6.9V_dev_t2_homekit_RF_2.0.19_s2_kvsABODE oz.

CVE-2020-8105 has been assigned by cve-requests@bitdefender.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Abode** - **iota All-In-One Security Kit** version < **1.0.2.23_6.9V_dev_t2_homekit_RF_2.0.19_s2_kvsABODE oz**

Vulnerability Patch/Work Around

An update to firmware version 1.0.2.23_6.9V_dev_t2_homekit_RF_2.0.19_s2_kvsABODE oz fixes the issue.

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
404 PAGE NOT FOUND	www.bitdefender.com text/html Inactive Link Not Archived	B MISC www.bitdefender.com/blog/labs/vulnerabilities-identified-in-theabode-iota-security-system-fake-image-injectioninto-timeline

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	Goabode	Iota All-in-one Security Kit	-	All	All	All
Operating System	Goabode	Iota All-in-one Security Kit Firmware	All	All	All	All

cpe:2.3:h:goabode:iota_all-in-one_security_kit:-:*:*:*:*:*:*:*:

cpe:2.3:o:goabode:iota_all-in-one_security_kit_firmware:*:*:*:*:*:*:*:*:

Discovery Credit

Bitdefender Labs

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2020-8105 : OS Command Injection vulnerability in the wirelessConnect handler of Abode iota All-In-One Security… twitter.com/i/web/status/1…	2021-12-20 13:45:36
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2020-8105 Description: OS Command Injection vulnerability in the wirelessCon… twitter.com/i/web/status/1…	2021-12-20 14:56:46
/r/netcve	CVE-2020-8105	2021-12-20 15:38:15
/r/Abode	Abode iota Threats and exploits.	2021-12-22 04:00:42

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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