

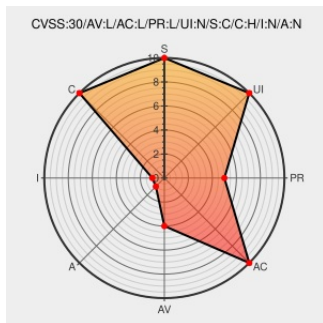


CVE-2019-5634

Published on: 08/22/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:59 PM UTC

CVE-2019-5634 - advisory for R7-2019-18.3

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

Certain versions of [Hickory Smart](#) from [Belwith-keeler](#) contain the following vulnerability:

An inclusion of sensitive information in log files vulnerability is present in Hickory Smart for Android mobile devices from Belwith Products, LLC. Communications to the internet API services and direct connections to the lock via Bluetooth Low Energy (BLE) from the mobile application are logged in a debug log on the Android device at

HickorySmartLog/Logs/SRDeviceLog.txt. This information was found stored in the Android device's default USB or SDcard storage paths and is accessible without rooting the device. This issue affects Hickory Smart for Android, version 01.01.43 and prior versions.

CVE-2019-5634 has been assigned by [cve@rapid7.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Belwith Products, LLC](#) - [Hickory Smart](#) version <= 01.01.43

CVSS3 Score: **4.3 - MEDIUM**

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

CVSS2 Score: **2.1 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Hickory Smart - Apps on Google Play	Product play.google.com text/html	 MISC play.google.com/store/apps/details?id=com.belwith.hickorysmart&hl=en_US
IoT Security: Hickory Smart Lock Vulnerability Disclosure Details	Third Party Advisory blog.rapid7.com text/html	 MISC blog.rapid7.com/2019/08/01/r7-2019-18-multiple-hickory-smart-lock-vulnerabilities/

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
Application	Belwith-keeler	Hickory Smart	All	All	All	All
cpe:2.3:a:belwith-keeler:hickory_smart:*:*:*:*:android:*:*:						

Discovery Credit

This issue was discovered and reported by Deral Heiland of Rapid7. It has been disclosed in accordance with Rapid7's vulnerability disclosure policy (<https://www.rapid7.com/disclosure/>).

[← 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](#)