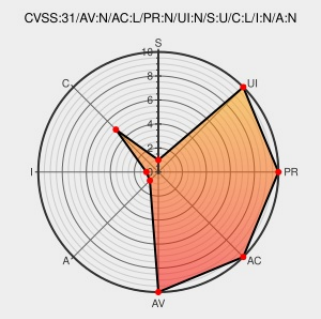
CVE-2020-8792

Published on: 05/04/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-8792

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



Certain versions of Oklok from Oklok Project contain the following vulnerability:

The OKLOK (3.1.1) mobile companion app for Fingerprint Bluetooth Padlock FB50 (2.3) has an information-exposure issue. In the mobile app, an attempt to add an already-bound lock by its barcode reveals the email address of the account to which the lock is bound, as well as the name of the lock. Valid barcode inputs can be easily guessed because barcode strings follow a predictable pattern. Correctly guessed valid barcode inputs entered through the app interface disclose arbitrary users' email addresses and lock names.

CVE-2020-8792 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.3 - MEDIUM

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

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
GitHub - fiercesoi/owpklok: PoC code for vulnerabilities on the OKLOK (3.1.1) mobile	Exploit	MISC

GitHub - fierceoj/ownklok: PoC code for vulnerabilities on the OKLOK (3.1.1) mobile companion app for Fingerprint Bluetooth Padlock FB50 (2.3).

Exploit
Third Party Advisory
github.com
text/html

MISC
github.com/fierceoj/ownklok

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	Oklok Project	Oklok	3.1.1	All	All	All
Application	Oklok Project	Oklok	3.1.1	All	All	All

cpe:2.3:a:oklok_project:oklok:3.1.1:*:*:*:*:iphone_os:*:*:

cpe:2.3:a:oklok_project:oklok:3.1.1:*:*:*:*:iphone_os:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→