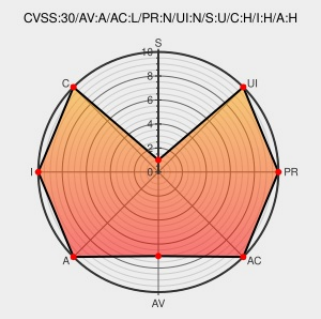
CVE-2017-17435

Published on: 12/06/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:27 PM UTC

CVE-2017-17435

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



Certain versions of Vt20i from Vaulteksafe contain the following vulnerability:

An issue was discovered in the software on Vaultek Gun Safe VT20i products, aka BlueSteal. An attacker can remotely unlock any safe in this product line without a valid PIN code. Even though the phone application requires it and there is a field to supply the PIN code in an authorization request, the safe does not check the PIN code, so an attacker can obtain authorization using any value. Once an attacker sees the Bluetooth Low Energy (BLE) advertisement for the safe, they need only to write a BLE characteristic to enable notifications, and send a crafted getAuthor packet that returns a temporary key, and an unlock packet including that temporary key. The safe then opens after the unlock packet is processed, with no verification of PIN or other credentials.

CVE-2017-17435 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 8.3 - HIGH

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

CVE References

Description	Tags	Link
BlueSteal: Popping GATT Safes - Two Six Labs | Advanced Analytics, Cyber Capabilities, Tactical Mobility Solutions for National Security	Third Party Advisory www.twosixlabs.com text/html	MISC www.twosixlabs.com/bluesteal-popping-gatt-safes/
404: Not Found	Vendor Advisory vaulteksafe.com text/html Inactive Link Not Archived	CONFIRM vaulteksafe.com/index.php/cve-2017-17435/

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	Vaulteksafe	Vt20i	-	All	All	All
Hardware	Vaulteksafe	Vt20i	-	All	All	All
Operating System	Vaulteksafe	Vt20i Firmware	-	All	All	All
Operating System	Vaulteksafe	Vt20i Firmware	-	All	All	All

cpe:2.3:h:vaulteksafe:vt20i:-:*:*:*:*:*:*:*:

cpe:2.3:h:vaulteksafe:vt20i:-:*:*:*:*:*:*:*:

cpe:2.3:o:vaulteksafe:vt20i_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:o:vaulteksafe:vt20i_firmware:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→