

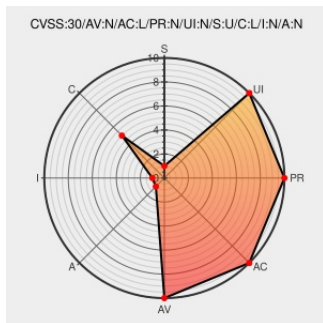


CVE-2019-5616

Published on: 03/15/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:00 PM UTC

CVE-2019-5616

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

Certain versions of [Scion-8](#) from [Broadcastboxes](#) contain the following vulnerability:

CircuitWerkes Sicon-8, a hardware device used for managing electrical devices, ships with a web-based front-end controller and implements an authentication mechanism in JavaScript that is run in the context of a user's web browser.

CVE-2019-5616 has been assigned by [cve@rapid7.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Because authentication is implemented as a JavaScript function that merely redirects the user away from the web app interface, rather than relying on session tokens or other more modern access controls, an attacker can navigate to `http://address:port/index.htm` using a standard web browser, and just before the page is fully rendered, hit the escape key to prevent the `window.location` redirect from executing. Once the page is rendered, the attacker can read all of the configured labels of a Sicon-8 device and retrieve the status of the labeled interfaces.

Vulnerability Patch/Work Around

Users of the Sicon-8 should not expose the web-based management console to untrusted networks.

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
CircuitWerkes Sicon-8 Client-Side Authentication Bypass Vuln Explained	Exploit Third Party Advisory blog.rapid7.com text/html	MISC blog.rapid7.com/2019/03/12/r7-2019-01-circuitwerkes-sicon-8-client-side-authentication-read-only-bypass-cve-2019-5616/

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 	Broadcastboxes	Scion-8	-	All	All	All
Hardware 	Broadcastboxes	Scion-8	-	All	All	All
Operating System	Broadcastboxes	Scion-8 Firmware	-	All	All	All
Operating System	Broadcastboxes	Scion-8 Firmware	-	All	All	All
cpe:2.3:h:broadcastboxes:scion-8:-:*:*:*:*:*:						
cpe:2.3:h:broadcastboxes:scion-8:-:*:*:*:*:*:						
cpe:2.3:o:broadcastboxes:scion-8_firmware:-:*:*:*:*:*:						
cpe:2.3:o:broadcastboxes:scion-8_firmware:-:*:*:*:*:*:						

Discovery Credit

This issue was discovered and reported by independent researcher Ph055a, and was validated and disclosed by Rapid7's Coordinated Vulnerability Disclosure program.

[← 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