

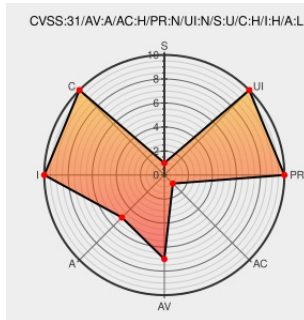


CVE-2020-9049

Published on: 11/19/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:13 PM UTC

CVE-2020-9049

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

Certain versions of [C-cure Web](#) from [Johnsoncontrols](#) contain the following vulnerability:

A vulnerability in specified versions of American Dynamics victor Web Client and Software House C•CURE Web Client could allow an unauthenticated attacker on the network to create and sign their own JSON Web Token and use it to execute an HTTP API Method without the need for valid authentication/authorization. Under certain

circumstances, this could be used by an attacker to impact system availability by conducting a Denial of Service attack.

CVE-2020-9049 has been assigned by productsecurity@jci.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Johnson Controls - victor Web Client version 5.6 and prior version <= 5.6**

Affected Vendor/Software: **Johnson Controls - C•CURE Web Client version 2.90 and prior (Note - This does not affect the new web-based C•CURE 9000 client that was introduced in C•CURE 9000 v2.90) version <= 2.90**

CVSS3 Score: **5.3 - MEDIUM**

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

CVSS2 Score: **5.7 - MEDIUM**

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	COMPLETE

CVE References

Description

Tags

Link

No Description Provided

Vendor Advisory

www.johnsoncontrols.com

text/html



CONFIRM

www.johnsoncontrols.com/cyber-solutions/security-advisories

Johnson Controls Sensormatic Electronics American Dynamics victor Web Client | CISA

Patch

Third Party Advisory

US Government Resource

us-cert.cisa.gov

text/html



CERT ICS-CERT Advisory

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	Johnsoncontrols	C-cure Web	All	All	All	All
Application	Johnsoncontrols	Victor Web	All	All	All	All
cpe:2.3:a:johnsoncontrols:c-cure_web:*:*:*:*:*:						
cpe:2.3:a:johnsoncontrols:victor_web:*:*:*:*:*:						

Discovery Credit

Joachim Kerschbaumer reported this vulnerability to Johnson Controls, Inc.

Social Mentions

Source	Title	Posted (UTC)
← 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