PRODUCT SECURITY ADVISORY

CARR-PSA-2025-04

November 18, 2025

Automated Logic WebCTRL® Software

Carrier i-Vu® Software

Overview

Automated Logic (ALC) manufactures Building Automation System (BAS) Products under multiple brands, including WebCTRL and i-Vu. These web-based platforms are designed to provide facility managers with tools that support occupant comfort, manage energy conservation measures, identify operational issues, and analyze system performance.

Researchers have identified two vulnerabilities affecting certain versions of WebCTRL and i-Vu: (1) a vulnerability that may allow attackers to exploit user sessions through a combination of Open Redirect and Cross-Site Scripting (XSS). [CVE-2024-8527] and (2) a vulnerability that allows for reflected XSS attacks due to a GET parameter not being sanitized [CVE-2024-8528].

Affected Products and Versions

Product	Version
Automated Logic WebCTRL® Server (all variants)	**6.1,6.5,7.0,8.0,8.5,9.0**
Carrier i-Vu® (all variants)	
Automated Logic SiteScan Web	
Automated Logic WebCTRL for OEMs (all variants)	

Vulnerability Details

CVE ID	CVSS	Severity
CVE-2024-8527	8.6	High
CVE-2024-8528	5.4	Medium

CVE ID: **CVE-2024-8527**

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:L

CWE-601: URL Redirection to Untrusted Site ('Open Redirect') - This weakness occurs when an application accepts a user-supplied URL and redirects the user to that URL without proper validation. Attackers can exploit this to redirect victims to malicious sites, often used in phishing or to bypass security controls.

CVE ID: **CVE-2024-8528**

CVSS:4.0/AV:L/AC:H/AT:P/PR:L/UI:P/VC:H/VI:H/VA:H/SC:L/SI:L/SA:L

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') - This is the most common form of XSS vulnerability. It happens when an application includes untrusted data in a web page without proper validation or escaping, allowing attackers to execute malicious scripts in the user's browser. Also (‘Reflected XSS') - This is used when a server application reads data directly from the HTTP request and reflects it back in the HTTP response.

Remediation

These vulnerabilities have been remediated in cumulative releases for versions 8.0, 8.5, and 9.0. Please be aware that WebCTRL and i-Vu versions 7.0, 6.5, and 6.1 are no longer supported. To safeguard against these vulnerabilities, upgrading to the latest WebCTRL and i-Vu software is strongly recommended.

About Carrier Global Product Cybersecurity

At Carrier, system and operational security is integral. The Product Security Incident Response Team (PSIRT) focuses on the identification, assessment, and disposition of the risks associated with security vulnerabilities within Carrier products, offerings, solutions, components and/or services. For more information about Global Product Security and PSIRT, please visit us at: https://www.corporate.carrier.com/product-security/

Or you may contact us at: productsecurity@carrier.com

Initial Publication Date	Last Publication Date
11-18-2025	11-18-2025