# PRODUCT SECURITY ADVISORY

CARR-PSA-2025-03

November 26, 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.

Security researchers have discovered vulnerabilities affecting certain versions of Automated Logic's BAS Products: (1) an Access Control Bypass vulnerability found in ALC WebCTRL® and Carrier i-Vu® in versions up to and including 8.5 allows a malicious actor to bypass intended access restrictions and expose sensitive information via the web-based building automation server. [CVE-2024-5539] and (2) a reflective cross-site scripting vulnerability found in ALC WebCTRL® and Carrier i-Vu® in versions older than 8.0 affects login panels allowing a malicious actor to compromise the client browser [CVE-2024-5540].

## Affected Products

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

## Vulnerability Details

| CVE ID | CVSS | Severity |
|---|---|---|
| CVE 2024-5539 | 9.2 | Critical |
| CVE 2024-5540 | 6.9 | Medium |

CVE ID: **CVE-2024-5539**

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

CWE-863 Incorrect Authorization: this software weakness where the system fails to perform adequate authorization checks, allows an actor to perform actions or access resources they are not entitled to. This can lead to bypassing access restrictions, privilege escalation, information exposure, or denial of service. The issue occurs when security policies are not properly enforced, leading to unauthorized access to sensitive information or functionality.

CVE ID: **CVE-2024-5540**

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

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.

## Remediation

These vulnerabilities have been remediated in cumulative releases for versions 8.0 and 8.5. 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 |
|---|---|
| 11-26-2025 | 11-26-2025 |