PRODUCT SECURITY ADVISORY

CARR-PSA-2025-05

November 26, 2025

Automated Logic WebCTRL®
Carrier i-Vu®

Overview

Automated Logic (ALC) manufactures Building Automation System (BAS) Products under multiple brands (WebCTRL® and i-Vu®). These BAS Products are a powerful web-based platform that provides facility managers with software tools to keep occupants comfortable, manage energy conservation measures, identify key operational problems, and analyze the results.

Researchers have reported a high-impact bug within WebCTRL and latest generation controllers (Gen5) which causes an array index out-of-range error, resulting in the cessation of an essential process within affected devices. The impact is the device may not be located by other devices on the network.

Affected Products

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)	
Latest generation controllers (Gen5)	Prior to version drv_gen5_108-04-20120

Vulnerability Details

CVE ID	CVSS v4.0	Severity
CVE-2025-0657	8.8	High

CVE ID: **CVE-2025-0657**

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

CWE-129: Improper Validation of Array Index: This weakness occurs when software uses an array index that has not been properly validated to ensure it falls within the valid bounds of the array. This can result in out-of-bounds access, leading to undefined behavior, memory corruption, or process termination.

CWE-248: Uncaught Exception: If the out-of-range access causes an exception that is not handled, leading to process termination.

Remediation

These vulnerabilities have been remediated in cumulative releases for versions 8.5, 9.0, and Gen5 driver version drv_gen5_108-04-20120 or later.

Support for versions 8.0, 7.0, 6.5, 6.1, 6.0 has expired.

Customers are advised to upgrade to the latest available version.

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