PRODUCT SECURITY ADVISORY

CARR-PSA-2024-04

November 21, 2024

Automated Logic WebCTRL Server

Carrier i-Vu

Automated Logic SiteScan Web

Automated Logic WebCTRL for OEMs

Overview

Automated Logic manufactures Building Automation System (BAS) Products under multiple brands (WebCTRL®, i-Vu, SiteScan Web, and WebCTRL for OEMs). 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.

Security researchers have discovered vulnerabilities affecting Automated Logic's BAS Products (WebCTRL® Server, i-Vu, SiteScan Web, and WebCTRL® for OEMs).

Successful exploitation of these vulnerabilities could allow an unauthenticated remote attacker to execute arbitrary commands on the server hosting the BAS Product.

It should be noted that the last support date for v7.0 was 1/27/2023.

Affected Products

BAS Product	Version
Automated Logic WebCTRL® Server (all variants)	see table below
Carrier i-Vu® (all variants)	
Automated Logic SiteScan Web	
Automated Logic WebCTRL for OEMs (all variants)	

Vulnerability Details

CVE ID	CVSS 4.0	Severity	Affected versions
CVE-2024-8525	Base Score 10.0	Critical	v7.0 only
CVE-2024-8526	Base Score 5.9	Medium	v7.0 only

CVE ID: **CVE-2024-8525**

CVSS v4.0 Base Score 10.0 Critical

Vector String : CVSS4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CWE-434 *Unrestricted Upload of File with Dangerous Type* vulnerability exists which could allow an unauthenticated user to upload files of dangerous types without restrictions, leading to remote command execution.

CVE ID: **CVE-2024-8526**

CVSS v4.0 Base Score 5.9 Medium

Vector String : CVSS4.0/AV:N/AC:L/AT:P/PR:N/UI:A/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

CWE-601 *URL Redirection to Untrusted Site ('Open Redirect')* vulnerability exists which could allow an attacker to send a maliciously crafted URL, which when visited by an authenticated WebCTRL user, results in the redirection of the user to a malicious webpage via "index.jsp"

Remediation

A software update fixing **CVE-2024-8525** *Unrestricted Upload of File with Dangerous Type* for v7.0 is available on the authorized dealer support site. Although a software update is available for this issue, the last support date for v7.0 was 1/27/2023 and it is recommended that customers upgrade their software to the latest supported version.

The **CVE-2024-8526** *Open Redirect* vulnerability was fixed at version 8.0 for all impacted products.

Mitigation

Customers are encouraged to follow Automated Logic's [Security Best Practices Checklists for Building Automation Systems (BAS)]() to ensure alignment with best practices installation guidelines.

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. PSIRT is a dedicated team of first responders responsible to deliver advanced support designed to contain and minimize the spread and impact of a product security event, incident, breach, and/or crises.

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
11-21-2024	11-21-2024