PRODUCT SECURITY ADVISORY

NOVEMBER 1, 2021

PSIRT Record Number
CARR-PSA-001-1121

Overview

The WebCTRL® building automation system is 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.

An open redirect vulnerability (CWE-601) was discovered affecting our Automated Logic's WebCTRL® server's Help pages. An open redirect vulnerability is when a malicious actor can redirect a web application's user to a malicious webpage in their control.

Impact

This vulnerability has a CVSS 3.1 score of 5.2 (Medium), with a vector string of CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N.

Affected Versions

The vulnerability effects all versions of WebCTRL® server prior to and including v7.0.

Solution

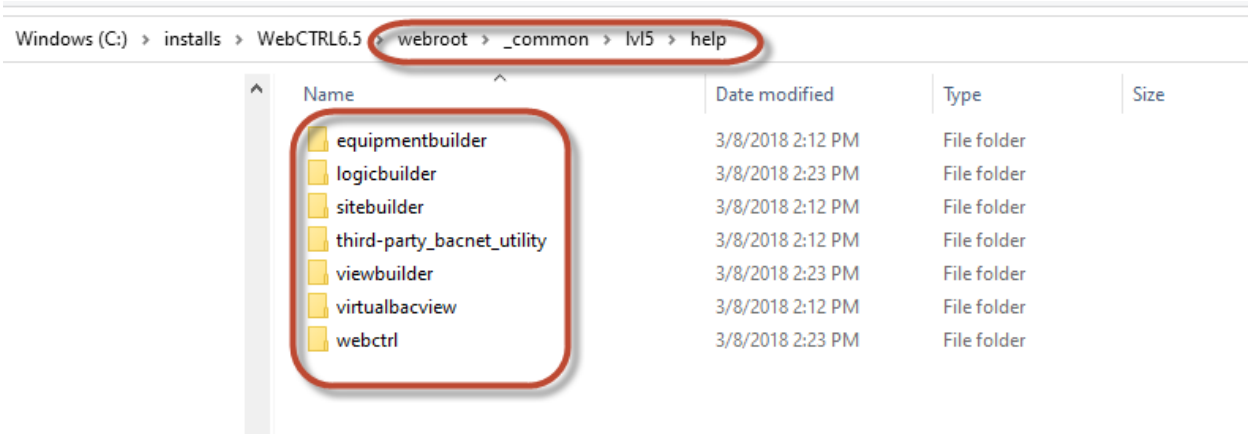
The vulnerability is mitigated by Content Security Policy in WebCTRL® server version 7.0 – “October 29, 2020 - cumulative patch” and later. It is recommended that customers upgrade their WebCTRL® software to the latest supported version.

Mitigation

As a manual work around users can add the CSP header/meta tag to each “index.htm” files in each of the directories under “<install_dir>/webroot/_common/lvl5/help/*”. These are the main index files for each help for each program/tool.

Example:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Frameset//EN"
  "http://www.w3.org/TR/html4/frameset.dtd">
<html>
<head>
<title>WebCTRL® v6.5 </title>
<meta name="Generator" content="AuthorIT">
<meta http-equiv="Content-Type" content="text/html; charset=ISO-
8859-1">
<meta name="SuperTitle" content="User's Guide" />
<meta http-equiv="Content-Security-Policy" content="default-src
'self'; img-src 'self' data:; font-src 'self' data:; script-src
'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-
inline'">
<script language="JavaScript">
function loadTopic(){
….
```



Support

Effective May 29, 2015

Automated Logic supports our current software product suites for one of the following, whichever is longer:

- 3 years after product launch, or
- 2 years after the last date the product is available for sale

Product	Launch Date	Last Sale Date	Last Support Date
v8.0	1/28/2021	-	-
v7.0	7/10/2018	1/27/2021	1/27/2023
v6.5	5/9/2016	7/9/2018	7/9/2020
v6.1	5/29/2015	5/6/2016	5/29/2018

https://www.automatedlogic.com/en/support/

Initial Publication Date	Last Published Date
November 1, 2021	November 1, 2021