America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Archived Content

In an effort to keep CISA.gov current, the archive contains outdated information that may not reflect current policy or programs.

ICS ADVISORY

Rockwell Automation Allen-Bradley CompactLogix Reflective Cross-Site Scripting Vulnerability (Update A)

Last Revised: October 30, 2018 **Alert Code:** ICSA-16-061-02

1. EXECUTIVE SUMMARY

- **CVSS v3 6.1**

--------- Begin Update A Part 1 of 5 --------

- **ATTENTION:** Exploitable remotely/low skill level to exploit/public exploits are available

--------- End Update A Part 1 of 5 ---------

- **Vendor:** Rockwell Automation
- **Equipment:** Allen-Bradley CompactLogix

- **Vulnerability:** Cross-site Scripting

2. UPDATE INFORMATION

This updated advisory is a follow-up to the original advisory titled ICSA-16-061-02 Rockwell Automation Allen-Bradley CompactLogix Reflective Cross-Site Scripting Vulnerability that was published March 1, 2016, on the NCCIC/ICS-CERT website.

3. RISK EVALUATION

Successful exploitation of this vulnerability could allow an attacker to inject arbitrary JavaScript into a user's web browser.

4. TECHNICAL DETAILS

4.1 AFFECTED PRODUCTS

Rockwell Automation reports the vulnerability affects the following versions of the Allen Bradley CompactLogix controller platform:

- 1769-L16ER-BB1B, Version 27.011 and prior,
- 1769-L18ER-BB1B, Version 27.011 and prior,
- 1769-L18ERM-BB1B, Version 27.011 and prior,
- 1769-L24ER-QB1B, Version 27.011 and prior,
- 1769-L24ER-QBFC1B, Version 27.011 and prior,
- 1769-L27ERM-QBFC1B, Version 27.011 and prior,
- 1769-L30ER, Version 27.011 and prior,
- 1769-L30ERM, Version 27.011 and prior,
- 1769-L30ER-NSE, Version 27.011 and prior,
- 1769-L33ER, Version 27.011 and prior,

- 1769-L33ERM, Version 27.011 and prior,
- 1769-L36ERM, Version 27.011 and prior,

--------- Begin Update A Part 2 of 5 --------

- 1769-L23E-QB1B, Version 20.018 and prior (discontinued as of June 2016),
- 1769-L23E-QBFC1B, Version 20.018 and prior (discontinued as of June 2016),
- 1756-EN2F,
  - Series A, all versions,
  - Series B, all versions,
- 1756-EN2T,
  - Series A, all versions,
  - Series B, all versions,
  - Series C, all versions,
  - Series D, Version 10.007 and prior,
- 1756-EN2TR,
  - Series A, all versions,
  - Series B, all versions,
- 1756-EN3TR, and
  - Series A, all versions.

--------- End Update A Part 2 of 5 ----------

4.2 VULNERABILITY OVERVIEW

4.2.1 IMPROPER NEUTRALIZATION OF INPUT DURING WEB PAGE GENERATION ('CROSS-SITE SCRIPTING') CWE-79 <https://cwe.mitre.org/data/definitions/79.html>

The vulnerability in the CompactLogix's web application allows an attacker to inject arbitrary JavaScript into a user's web browser. The target of this type of attack is not the CompactLogix itself. Instead, the CompactLogix is a vehicle used to deliver an attack to the

web browser.

CVE-2016-2279 has been assigned to this vulnerability. A CVSS v3 base score of 6.1 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N <https://www.first.org/cvss/calculator/3.0#cvss:3.0/av:n/ac:l/pr:n/ui:r/s:c/c:l/i:l/a:n>).

4.3 BACKGROUND

- **CRITICAL INFRASTRUCTURE SECTORS:** Chemical, Critical Manufacturing, Energy, Food and Agriculture, Water and Wastewater Systems
- **COUNTRIES/AREAS DEPLOYED:** Worldwide
- **COMPANY HEADQUARTERS LOCATION:** United States

4.4 RESEARCHER

--------- Begin Update A Part 3 of 5 ---------

Aditya Sood and Venkatesh Sivakumar (@PranavVenkatS) reported this vulnerability to NCCIC.

--------- End Update A Part 3 of 5 ---------

5. MITIGATIONS

Rockwell Automation recommends that users of 1769-L23E-QB1B migrate to 1769-L24ER-BB1B and users of 1769-L23E-QBFC1B migrate to 1769-L24ER-QBFC1B.

--------- Begin Update A Part 4 of 5 ---------

For 1756-EN2F Series C, 1756-EN2T Series D, 1756-EN2TR Series C, and 1756-EN3TRSeries B, Rockwell Automation recommends users apply FRN 10.010 or later available at:

https://compatibility.rockwellautomation.com/Pages/MultiProductDownload.aspx?Keyword=1756-EN3TR&crumb=112

For earlier versions: users using previous series of the affected 1756 EtherNet/IP catalog numbers are urged to assess their risk and, if necessary, contact their local distributor or sales office in order to upgrade to a newer product line that contains the relevant mitigations.

--------- End Update A Part 4 of 5 ---------

For the other affected versions listed above, Rockwell Automation recommends users apply firmware Version 28.011+ available at:

http://compatibility.rockwellautomation.com/Pages/MultiProductDownload.aspx?famID=4

For more detailed information, please see Rockwell Automation's security notification (KB731098), available at the following URL with a valid account:

https://rockwellautomation.custhelp.com/app/answers/detail/a_id/731098

<https://rockwellautomation.custhelp.com/app/answers/detail/a_id/731098>

--------- Begin Update A Part 5 of 5 ---------

Rockwell Automation also recommends the following security practices:

- Do not click on or open URL links from untrusted sources.
- Employ training and awareness programs to educate users on the warning signs of a phishing or social engineering attack.
- Use trusted software, software patches, antivirus/antimalware programs and interact only with trusted websites and attachments.
- Employ training and awareness programs to educate users on the warning signs of a phishing or social engineering attack.
- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet
- Locate control system networks and devices behind firewalls, and isolate them from the business network.

- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

NCCIC reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

NCCIC also provides a section for control systems security recommended practices </ics/content/recommended-practices> on the ICS-CERT web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies </sites/default/files/recommended_practices/nccic_ics-cert_defense_in_depth_2016_s508c.pdf>.

Additional mitigation guidance and recommended practices are publicly available on the ICS-CERT website </ics/> in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies </ics/tips/ics-tip-12-146-01b>.

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to NCCIC for tracking and correlation against other incidents.

NCCIC also recommends that users take the following measures to protect themselves from social engineering attacks:

- Do not click web links or open unsolicited attachments in email messages.
- Refer to Recognizing and Avoiding Email Scams </reading_room/emailscams_0905.pdf> for more information on avoiding email scams.
- Refer to Avoiding Social Engineering and Phishing Attacks </cas/tips/st04-014.html> for more information on social engineering attacks.

--------- End Update A Part 5 of 5 ---------

Vendor

- Rockwell Automation

Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov

CISA.gov