America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

ICS ADVISORY

Rockwell Automation Allen-Bradley MicroLogix 1100 and 1400

Last Revised: May 23, 2017 **Alert Code:** ICSA-17-115-04

CVSS v3 9.8

ATTENTION: Remotely exploitable/low skill level to exploit.

Vendor: Rockwell Automation

Equipment: Allen-Bradley MicroLogix 1100 and 1400

Vulnerabilities: Predictable Value Range from Previous Values; Reusing a Nonce, Key Pair in Encryption; Information Exposure; Improper Restriction of Excessive Authentication Attempts; Weak Password Requirements

REPOSTED INFORMATION

This advisory was originally posted to the NCCIC Portal on April 25, 2017, and is being released to the ICS-CERT web site.

AFFECTED PRODUCTS

The following versions of the Allen-Bradley MicroLogix 1100 programmable-logic controller are affected:

- 1763-L16AWA, Series A and B, Version 16.00 and prior versions;
- 1763-L16BBB, Series A and B, Version 16.00 and prior versions;
- 1763-L16BWA, Series A and B, Version 16.00 and prior versions; and
- 1763-L16DWD, Series A and B, Version 16.00 and prior versions.

The following versions of the Allen-Bradley MicroLogix 1400 programmable logic controller are affected:

- 1766-L32AWA, Series A and B, Version 16.00 and prior versions;
- 1766-L32BWA, Series A and B, Version 16.00 and prior versions;
- 1766-L32BWAA, Series A and B, Version 16.00 and prior versions;
- 1766-L32BXB, Series A and B, Version 16.00 and prior versions;
- 1766-L32BXBA, Series A and B, Version 16.00 and prior versions; and
- 1766-L32AWAA, Series A and B, Version 16.00 and prior versions.

IMPACT

Successful exploitation of these vulnerabilities may allow a remote attacker to gain unauthorized access to the affected programmable logic controllers and to spoof or disrupt TCP connections.

MITIGATION

Rockwell Automation has released a new firmware version for the Allen-Bradley MicroLogix 1400 Series B controllers, FRN 21.00, to address the identified vulnerabilities. Rockwell Automation encourages users to apply the latest firmware versions that address the identified vulnerabilities.

Rockwell Automation's new firmware version for the Allen-Bradley MicroLogix 1400 Series B controllers, FRN 21.00, is available at the following location:

http://compatibility.rockwellautomation.com/Pages/MultiProductDownload.aspx?Keyword=1766-Lxx&crumb=112

There are no firmware versions to address these vulnerabilities in the Allen-Bradley MicroLogix 1100 or MicroLogix 1400 Series A controllers, but Rockwell Automation has offered some compensating controls. Rockwell Automation reports that users can disable the web server on the Allen-Bradley MicroLogix 1100 and 1400 Series A controllers to protect against the exploitation of the improper restriction of excessive authentication attempts and weak password requirements vulnerabilities.

Rockwell Automation recommends that if it is not needed, users should consider disabling the web server to further mitigate these threats.

- Disable the web server on the MicroLogix 1100 and 1400 controllers, if not needed, as it is enabled by default. See Knowledge Base article: 732398 for detailed instructions on disabling the web server. The Web Server Tech Note, KB: 732398 – How to Disable the Web Server in MicroLogix 1100 and 1400 is available at the following URL with a valid account:

https://rockwellautomation.custhelp.com/app/answers/detail/a_id/732398

<https://rockwellautomation.custhelp.com/app/answers/detail/a_id/732398>

- Set the mode to RUN via LCD soft keyswitch to prohibit any re-enabling of the web server while the keyswitch is in this mode.

NCCIC/ICS-CERT recommends that users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should:

- 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 remote 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.

ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

ICS-CERT 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 in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies </ics/tips/ics-tip-12-146-01b>, that is available for download from the ICS-CERT web site </ics/>.

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

In addition, ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks:

1. Do not click web links or open unsolicited attachments in email messages.

2. Refer to Recognizing and Avoiding Email Scams </reading_room/emailscams_0905.pdf> for more information on avoiding email scams.
3. Refer to Avoiding Social Engineering and Phishing Attacks </cas/tips/st04-014.html> for more information on social engineering attacks.

No known public exploits specifically target these vulnerabilities.

VULNERABILITY OVERVIEW

PREDICTABLE VALUE RANGE FROM PREVIOUS VALUES CWE-343

<https://cwe.mitre.org/data/definitions/343.html>

Insufficiently random TCP initial sequence numbers are generated, which may allow an attacker to predict the numbers from previous values. This may allow an attacker to spoof or disrupt TCP connections, resulting in a denial of service for the target device.

CVE-2017-7901 has been assigned to this vulnerability. A CVSS v3 base score of 5.4 has been assigned; the CVSS vector string is (AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:L <https://www.first.org/cvss/calculator/3.0#cvss:3.0/av:n/ac:h/pr:n/ui:n/s:c/c:n/i:l/a:l>).

REUSING A NONCE, KEY PAIR IN ENCRYPTION CWE-323 <https://cwe.mitre.org/data/definitions/323.html>

The affected product reuses nonces, which may allow an attacker to capture and replay a valid request until the nonce is changed.

CVE-2017-7902 has been assigned to this vulnerability. A CVSS v3 base score of 5.4 has been assigned; the CVSS vector string is (AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L <https://www.first.org/cvss/calculator/3.0#cvss:3.0/av:n/ac:l/pr:n/ui:r/s:u/c:n/i:l/a:l>).

INFORMATION EXPOSURE CWE-200

<https://cwe.mitre.org/data/definitions/200.html>

User credentials are sent to the web server using the HTTP GET method, which may result in the credentials being logged. This could make user credentials available for unauthorized retrieval.

CVE-2017-7899 has been assigned to this vulnerability. A CVSS v3 base score of 3.1 has been assigned; the CVSS vector string is (AV:L/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N <https://www.first.org/cvss/calculator/3.0#cvss:3.0/av:l/ac:l/pr:h/ui:r/s:u/c:l/i:l/a:n>).

IMPROPER RESTRICTION OF EXCESSIVE AUTHENTICATION ATTEMPTS CWE-307

<https://cwe.mitre.org/data/definitions/307.html>

There are no penalties for repeatedly entering incorrect passwords.

CVE-2017-7898 has been assigned to this vulnerability. A CVSS v3 base score of 9.8 has been assigned; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H <https://www.first.org/cvss/calculator/3.0#cvss:3.0/av:n/ac:l/pr:n/ui:n/s:u/c:h/i:h/a:h>).

WEAK PASSWORD REQUIREMENTS CWE-521

<https://cwe.mitre.org/data/definitions/521.html>

The affected products use a numeric password with a small maximum character size for the password.

CVE-2017-7903 has been assigned to this vulnerability. A CVSS v3 base score of 9.8 has been assigned; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H <https://www.first.org/cvss/calculator/3.0#cvss:3.0/av:n/ac:l/pr:n/ui:n/s:u/c:h/i:h/a:h>).

RESEARCHER

These vulnerabilities were reported to ICS-CERT by Rockwell Automation, David Formby and Raheem Beyah of Georgia Tech and Fortiphyd Logic, Inc. Rockwell Automation also reported a vulnerability that was initially identified by Ilya Karpov of Positive Technologies.

BACKGROUND

Critical Infrastructure Sectors: Food and Agriculture, Water and Wastewater Systems

Countries/Areas Deployed: Worldwide

Company Headquarters Location: Milwaukee, Wisconsin

Vendor

- Rockwell Automation

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
An official website of the U.S. Department of Homeland Security

About CISA </about>

Budget and Performance <https://www.dhs.gov/performance-financial-reports>

DHS.gov <https://www.dhs.gov>

FOIA Requests <https://www.dhs.gov/foia>

No FEAR Act </no-fear-act>

Office of Inspector General <https://www.oig.dhs.gov/>

Privacy Policy </privacy-policy>

Subscribe

The White House <https://www.whitehouse.gov/>

USA.gov <https://www.usa.gov/>

Website Feedback </forms/feedback>