TLP:WHITE

NCCIC

Advisory (ICSA-16-224-01)

Rockwell Automation MicroLogix 1400 SNMP Credentials Vulnerability

Original release date: August 11, 2016 | Last revised: August 23, 2018

OVERVIEW

Cisco Talos, Cisco Systems, Inc.'s security intelligence and research group reported to Rockwell Automation that an undocumented and privileged Simple Network Management Protocol (SNMP) community string exists in MicroLogix 1400 programmable logic controllers (PLC). Rockwell Automation has released mitigation strategies to protect against this threat.

This vulnerability could be exploited remotely.

AFFECTED PRODUCTS

Rockwell Automation reports that the vulnerability affects all versions of the following products:

- 1766-L32BWA,
- 1766-L32AWA ,
- 1766-L32BXB,
- 1766-L32BWAA,
- 1766-L32AWAA, and
- 1766-L32BXBA.

IMPACT

This vulnerability may allow an attacker to make unauthorized changes to the product's configuration, including firmware updates.

Impact to individual organizations depends on many factors that are unique to each organization. NCCIC/ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation.

BACKGROUND

Rockwell Automation, which is a US-based company, provides industrial automation control and information products worldwide across a wide range of industries.

TLP:WHITE

The affected products, MicroLogix, are PLCs. According to Rockwell Automation, these products are deployed across several sectors, including Chemical, Critical Manufacturing, Food and Agriculture, Water and Wastewater Systems, and others. Rockwell Automation estimates that these products are used in Germany, Czech Republic, France, Poland, Denmark, Hungary, Italy, and other countries in Europe, as well as in the United States, Korea, China, Japan, and in Latin American countries.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

EXECUTION WITH UNNECESSARY PRIVILEGES[a]

SNMP is a standard protocol employed by many types of internet protocol based products and allows centralized and remote device management capabilities. One of the many standard SNMP capabilities enables users to manage the product's firmware, including the capability of applying firmware updates to the product. The MicroLogix 1400 utilizes this standard SNMP capability as its official mechanism for applying firmware updates to the product.

CVE-2016-5645[b] has been assigned to this vulnerability. A CVSS v3 base score of 7.3 has been calculated; the CVSS vector string is (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).[c]

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability could be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

An attacker with a low skill would be able to exploit this vulnerability.

MITIGATION

Due to the nature of this product's firmware update process, this capability cannot be removed from the product. Instead, mitigations are offered to reduce risk of this capability being used by a malicious actor.

Rockwell Automation recommends that users using affected versions of the MicroLogix 1400 evaluate and deploy the risk mitigation strategies listed below. When possible, multiple strategies should be employed simultaneously.

- Utilize the product's "RUN" keyswitch setting to prevent unauthorized and undesired firmware update operations and other disruptive configuration changes.
- Utilize proper network infrastructure controls, such as firewalls, to help ensure that SNMP requests from unauthorized sources are blocked. See KB496391[d] for more information on blocking access to SNMP services.
- Disable the SNMP service on this product. The SNMP service is enabled by default. See Page 128 in the MicroLogix 1400 product manual[e] for detailed instructions on enabling and disabling SNMP.
  - Note: It will be necessary to re-enable SNMP to update firmware on this product. After the upgrade is complete, disable the SNMP service once again.
  - Note: Changing the SNMP community strings is not an effective mitigation.

TLP:WHITE

- 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 a 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 on the ICS-CERT web page at: http://ics-cert.us-cert.gov/content/recommended-practices. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

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, that is available for download from the ICS-CERT web site (http://ics-cert.us-cert.gov/).

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.

---

a. CWE-250: Execution with Unnecessary Privileges, http://cwe.mitre.org/data/definitions/250.html, web site last accessed August 11, 2016.

b. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-5645, NIST uses this advisory to create the CVE web site report. This web site will be active sometime after publication of this advisory.

c. CVSS Calculator, https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S..., web site last accessed August 11, 2016.

d. KB496391, https://rockwellautomation.custhelp.com/app/answers/detail/a_id/496391, web site last accessed August 11, 2016.

e. MicroLogix 1400 Product Manual, http://literature.rockwellautomation.com/idc/groups/literature/documents..., web site last accessed August 11, 2016.

Contact Information

For any questions related to this report, please contact the NCCIC at:

Email: NCCICCUSTOMERSERVICE@hq.dhs.gov
Toll Free: 1-888-282-0870

For industrial control systems cybersecurity information: http://ics-cert.us-cert.gov
or incident reporting: https://ics-cert.us-cert.gov/Report-Incident?

The NCCIC continuously strives to improve its products and services. You can help by choosing one of the links below to provide feedback about this product.

TLP:WHITE

TLP:WHITE

TLP:WHITE