Advisory (ICSA-14-254-02)

Rockwell Micrologix 1400 DNP3 DOS Vulnerability

Original release date: September 30, 2014

OVERVIEW

This advisory was originally posted to the US-CERT secure Portal library on September 11, 2014, and is being released to the NCCIC/ICS-CERT web site.

Independent researcher Matthew Luallen of CYBATI has identified a denial-of-service (DoS) vulnerability to the DNP3 implementation of the Allen-Bradley MicroLogix 1400 controller platform. Rockwell Automation has produced a firmware revision that mitigates this vulnerability.

This vulnerability could be exploited remotely.

AFFECTED PRODUCTS

The following Allen-Bradley MicroLogix 1400 controller platforms are affected:

- 1766-Lxxxxx Series A FRN 7 and earlier, and
- 1766-Lxxxxx Series B FRN 15.000 and earlier.

IMPACT

Successful exploitation of this vulnerability results in a disruption of the DNP3 application layer process and a loss of product communication and availability on the network, thereby resulting in a DoS condition. Product recovery from the DoS condition requires a power cycle.

Impact to individual organizations depends on many factors that are unique to each organization. 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.

The affected products, MicroLogix, are programmable logic controllers (PLCs). According to Rockwell Automation, these products are deployed across several sectors including Chemical, Critical Manufacturing, Food and Agriculture, and 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 the United States, Korea, China, Japan, and Latin American countries.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

IMPROPER INPUT VALIDATION[a]

DNP3 communication is disabled by default in the MicroLogix 1400 product. If the DNP3 capability is enabled, specific versions of the product become susceptible to a DoS attack. The DoS attack can be triggered when the product receives a particular series of malformed packets over its Ethernet or local serial ports that are directed at the link layer DNP3 header.

CVE-2014-5410[b] has been assigned to this vulnerability. A CVSS v2 base score of 7.1 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:N/I:N/A:C).[c]

VULNERABILITY DETAILS

EXPLOITAVILITY

This vulnerability could be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

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

MITIGATION

Rockwell Automation has released a new version of MicroLogix 1400 Series B firmware to address the vulnerability and reduce associated risk to successful exploitation. Subsequent versions of MicroLogix 1400 Series B firmware and newer will incorporate these same enhancements.

Rockwell Automation recommends the following immediate mitigation strategies (when possible, multiple strategies should be employed simultaneously):

- Upgrade all MicroLogix 1400 Series B controllers to Series B FRN 15.001 or higher. Current firmware for the MicroLogix 1400 Series B platform can be obtained at the following web address:

http://www.rockwellautomation.com/rockwellautomation/support/pcdc.page

Users with Series A and Series B controllers are also recommended to apply the following risk mitigations:

- Do not enable DNP3 communication in the product unless required.
- Where appropriate, prohibit DNP3 communication that originates outside the perimeter of the Manufacturing Zone from entry into the Zone by blocking communication directed at Ethernet communication Port 20000/TCP* and 20000/UDP* using appropriate security technology (e.g., a firewall, UTM devices, or other security appliance)

  *Note: Ports 20000/TCP and 20000/UDP are factory defaults as per the DNP3 specification but can be reconfigured by the product owner.

- Employ firewalls with ingress/egress filtering, intrusion detection/prevention systems, and validate all configurations. Evaluate firewall configurations to ensure othe appropriate inbound and outbound traffic is blocked.
- Restrict physical and electronic access to automation products, networks, and systems to only those individuals authorized to be in contact with control system equipment.
- Employ layered security, defense-in-depth methods and network segregation and segmentation practices in system design to restrict and control access to individual products and control networks. Refer to http://www.ab.com/networks/architectures.html for comprehensive information about implementing validated architectures designed to deliver these measures.

Please refer to Rockwell Automation's product disclosure (AID 620295) for more information on this topic available at:

https://rockwellautomation.custhelp.com/app/answers/detail/a_id/620295

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

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

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 (www.ics-cert.org).

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-20: Improper Input Validation, http://cwe.mitre.org/data/definitions/20.html, web site last accessed September 30, 2014.

b. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-5410, 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, http://nvd.nist.gov/cvss.cfm?version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:C , web site last accessed September 30, 2014.

Contact Information

For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@hq.dhs.gov
Toll Free: 1-877-776-7585
International Callers: (208) 526-0900

For industrial control systems security information and incident reporting: http://ics-cert.us-cert.gov

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