ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-13-011-03—ROCKWELL AUTOMATION CONTROLLOGIX MULTIPLE PLC VULNERABILITIES

January 11, 2013

OVERVIEW

This advisory is a follow up to the original alert titled ICS-Alert-12-020-02A—Rockwell Automation ControlLogix Multiple PLC Vulnerabilities[a] that was published February 14, 2012, on the ICS-CERT Web page.

Independent researcher Rubén Santamarta of IOActive identified multiple vulnerabilities in Rockwell Automation's ControlLogix PLC and released proof-of-concept (exploit) code at the Digital Bond S4 Conference on January 19, 2012. The vulnerabilities are exploitable by transmitting arbitrary commands from a control interface to the programmable logic controller (PLC) or network interface card (NIC). The information was released without coordination with either the vendor or ICS-CERT. Rockwell Automation released firmware patches on July 18, 2012, that resolve the following vulnerabilities. There have been no updates from Rockwell since these patches were released. Exploitation of these vulnerabilities could allow loss of confidentiality, integrity, and availability of the device.

These vulnerabilities could be exploited remotely. Exploits that target these vulnerabilities are publicly available.

AFFECTED PRODUCTS

The following Rockwell products are affected:

- All EtherNet/IP products that conform to the CIP and EtherNet/IP specifications,
- 1756-ENBT, 1756-EWEB, 1768-ENBT, 1768-EWEB communication modules,
- CompactLogix L32E and L35E controllers,
- 1788-ENBT FLEXLogix adapter,
- 1794-AENTR FLEX I/O EtherNet/IP adapter,

[a] ICS-Alert-12-020-02A—Rockwell Automation ControlLogix Multiple PLC Vulnerabilities, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-12-020-02A.pdf, Web site last accessed January 11, 2013.

- ControlLogix, CompactLogix, GuardLogix, and SoftLogix, Version 18 and prior,
- CompactLogix and SoftLogix controllers, Version 19 and prior,
- ControlLogix and GuardLogix controllers, Version 20 and prior,
- MicroLogix 1100, and
- MicroLogix 1400.

IMPACT

Successful exploitation of these vulnerabilities may result in a denial-of-service (DoS) condition, controller fault, or enable a Man-in-the-Middle (MitM) attack, or Replay attack.

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

BACKGROUND

Rockwell Automation provides industrial automation control and information products worldwide, across a wide range of industries.

The affected products are PLCs and communication modules. According to Rockwell Automation, these products are deployed across several sectors including agriculture and food, water, chemical, manufacturing and others. According to Rockwell's Web site, these products are used in France, Italy, the Netherlands, and other countries in Europe, as well as the United States, Korea, China, Japan, and Latin American countries.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

IMPROPER ACCESS CONTROL—CHANGE IP[b]

When an affected product receives a valid CIP message from an unauthorized or unintended source to Port 2222/TCP, Port 2222/UDP, Port 44818/TCP, or Port 44818/UDP that changes the product's configuration and network parameters, a DoS condition can occur. This situation could cause loss of availability and a disruption of communication with other connected devices.

[b] CWE, http://cwe mitre.org/data/definitions/284.html, CWE-284: Improper Access Control, Web site last accessed January 09, 2013.

CVE-2012-6439[c] has been assigned to this vulnerability. A CVSS v2 base score of 8.5 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:P/A:C).[d]

IMPROPER ACCESS CONTROL—RESET[e]

When an affected product receives a valid CIP message from an unauthorized or unintended source to Port 2222/TCP, Port 2222/UDP, Port 44818/TCP, or Port 44818/UDP that instructs the product to reset, a DoS can occur. This situation could cause loss of availability and a disruption of communication with other connected devices.

This vulnerability was discovered by Rockwell Automation engineers as they were investigating other vulnerabilities reported at the Digital Bond S4 2012 Conference.

CVE-2012-6442[f] has been assigned to this vulnerability. A CVSS v2 base score of 7.8 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:N/A:C).[g]

IMPROPER ACCESS CONTROL—STOP[h]

When an affected product receives a valid CIP message from an unauthorized or unintended source to Port 2222/TCP, Port 2222/UDP, Port 44818/TCP, or Port 44818/UDP that instructs the CPU to stop logic execution and enter a fault state, a DoS can occur. This situation could cause loss of availability and a disruption of communication with other connected devices.

CVE-2012-6435[i] has been assigned to this vulnerability. A CVSS v2 base score of 7.8 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:N/A:C).[j]

[c] NVD, http://web nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-6439, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

[d] CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:N/I:P/A:C), Web site last visited January 11, 2013.

[e] CWE, http://cwe.mitre.org/data/definitions/284 html, CWE-284: Improper Access Control, Web site last accessed January 11, 2013.

[f] NVD, http://web.nvd nist.gov/view/vuln/detail?vulnId=CVE-2012-6442, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

[g] CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:N/I:N/A:C), Web site last visited January 11, 2013.

[h] CWE, http://cwe mitre.org/data/definitions/284.html, CWE-284: Improper Access Control, Web site last accessed January 11, 2013.

[i] NVD, http://web nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-6435, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

[j] CVSS Calculator, http://nvd nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:N/I:N/A:C), Web site last visited January 11, 2013.

INFORMATION EXPOSURE[k]

An information exposure of confidential information results when the device receives a specially crafted CIP packet to Port 2222/TCP, Port 2222/UDP, Port 44818/TCP, or Port 44818/UDP. Successful exploitation of this vulnerability could cause loss of confidentiality.

This vulnerability was discovered by Rockwell Automation engineers as they were investigating other vulnerabilities reported at the Digital Bond S4 2012 Conference.

CVE-2012-6441[l] has been assigned to this vulnerability. A CVSS v2 base score of 5.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:P/I:N/A:N).[m]

IMPROPER INPUT VALIDATION—NIC[n]

The device does not properly validate the data being sent to the buffer. An attacker can send a malformed CIP packet to Port 2222/TCP, Port 2222/UDP, Port 44818/TCP, or Port 44818/UDP, which creates a buffer overflow and causes the NIC to crash. Successful exploitation of this vulnerability could cause loss of availability and a disruption in communications with other connected devices.

CVE-2012-6438[o] has been assigned to this vulnerability. A CVSS v2 base score of 7.8 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:N/A:C).[p]

IMPROPER INPUT VALIDATION—CPU[q]

The device does not properly validate the data being sent to the buffer. An attacker can send a malformed CIP packet to Port 2222/TCP, Port 2222/UDP, Port 44818/TCP, or Port 44818/UDP, which creates a buffer overflow and causes the CPU to crash. Successful exploitation of this

[k] CWE, http://cwe mitre.org/data/definitions/200.html, CWE-200: Information Exposure, Web site last accessed January 11, 2013.

[l] NVD, http://web nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-6441, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

[m] CVSS Calculator, http://nvd nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:P/I:N/A:N), Web site last visited January 11, 2013.

[n] CWE, http://cwe mitre.org/data/definitions/20 html, CWE-20: Improper Input Validation, Web site last accessed January 11, 2013.

[o] NVD, http://web.nvd nist.gov/view/vuln/detail?vulnId=CVE-2012-6438, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

[p] CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:N/I:N/A:C), Web site last visited January 11, 2013.

[q] CWE, http://cwe mitre.org/data/definitions/20.html, CWE-20: Improper Input Validation, Web site last accessed January 11, 2013.

vulnerability could cause loss of availability and a disruption in communications with other connected devices.

CVE-2012-6436[r] has been assigned to this vulnerability. A CVSS v2 base score of 7.8 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:N/A:C).[s]

AUTHENTICATION BYPASS BY CAPTURE—REPLAY[t]

The Web server password authentication mechanism used by the products is vulnerable to a MitM and Replay attack. Successful exploitation of this vulnerability will allow unauthorized access of the product's Web server to view and alter product configuration and diagnostics information.

This vulnerability was discovered by Rockwell Automation engineers as they were investigating other vulnerabilities reported at the Digital Bond S4 2012 Conference.

CVE-2012-6440[u] has been assigned to this vulnerability. A CVSS v2 base score of 9.3 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:C/I:C/A:C).[v]

IMPROPER AUTHENTICATION—FIRMWARE UPLOAD[w]

The device does not properly authenticate users and the potential exists for a remote user to upload a new firmware image to the Ethernet card, whether it is a corrupt or legitimate firmware image. Successful exploitation of this vulnerability could cause loss of availability, integrity, and confidentiality and a disruption in communications with other connected devices.

CVE-2012-6437[x] has been assigned to this vulnerability. A CVSS v2 base score of 10.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:C/A:C).[y]

[r] NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-6436, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

[s] CVSS Calculator, http://nvd nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:N/I:N/A:C), Web site last visited January 11, 2013.

[t] CWE, http://cwe.mitre.org/data/definitions/294 html, CWE-294: Authentication Bypass by Capture-replay, Web site last accessed January 11, 2013.

[u] NVD, http://web.nvd nist.gov/view/vuln/detail?vulnId=CVE-2012-6440, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

[v] CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:N/C:C/I:C/A:C), Web site last visited January 11, 2013.

[w] CWE, http://cwe mitre.org/data/definitions/284.html, CWE-284: Improper Access Control, Web site last accessed January 11, 2013.

[x] NVD, http://web.nvd nist.gov/view/vuln/detail?vulnId=CVE-2012-6437, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities could be exploited remotely.

EXISTENCE OF EXPLOIT

Exploits that target these vulnerabilities are publicly available.

DIFFICULTY

An attacker with a low-medium skill would be able to exploit these vulnerabilities.

MITIGATION

According to Rockwell, any of the above products that become affected by a vulnerability can be reset by rebooting or power cycling the affected product. After the reboot, the affected product may require some reconfiguration.

To mitigate the vulnerabilities, Rockwell has developed and released security patches on July 18, 2012, to address each of the issues. To download and install the patches please refer to Rockwell's Advisories at:

https://rockwellautomation.custhelp.com/app/answers/detail/a_id/470154

https://rockwellautomation.custhelp.com/app/answers/detail/a_id/470155

https://rockwellautomation.custhelp.com/app/answers/detail/a_id/470156

For more information on security with Rockwell Automation products, please refer to Rockwell's Security Advisory Index at: http://rockwellautomation.custhelp.com/app/answers/detail/a_id/54102.

Rockwell recommends updating to the newest firmware patches to fix the vulnerabilities, but if not able to do so right away, then Rockwell advises immediately employing the following mitigations for each of the affected products.

y. CVSS Calculator, http://nvd nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:C/I:C/A:C), Web site last visited January 11, 2013.

To mitigate the vulnerabilities pertaining to receiving valid CIP packets:

1. Block all traffic to the Ethernet/IP or other CIP protocol-based devices from outside the Manufacturing Zone by restricting or blocking access to TCP and UDP Ports 2222 and 44818 using appropriate security technology such as a firewall or Unified Threat Management (UTM).
2. Employ a UTM appliance that specifically supports CIP message filtering.

To mitigate the vulnerability pertaining to the corrupted firmware update:

1. At this time, Rockwell is still evaluating the feasibility of creating an update for the 1756-ENBT communication module to include a digital signature validation mechanism on the firmware.
2. Until Rockwell creates an update, concerned customers are recommended to employ good security design practices and consider using the more contemporary 1756-EN2T Ethernet/IP communication modules for the ControlLogix platform. The 1756-EN2T has been able to validate digital signatures since firmware Release 5.028.

To mitigate receiving malformed CIP packets that can cause the controller to enter a fault state:

1. Where possible, Rockwell recommends users to upgrade the affected products to Logix Release V20 and higher.

To mitigate receiving valid CIP packets that instruct the controller to stop logic execution and enter a fault state:

1. Where possible, upgrade CompactLogix and SoftLogix affected products to Logix Release V20 or higher.
2. Where possible, upgrade ControlLogix and GuardLogix affected products to Logix Release v20.012 or higher.
3. Block all traffic to the Ethernet/IP or other CIP protocol devices as directed above.
4. Employ a UTM as directed above.

To mitigate the vulnerability with the Web server password authentication mechanism:

1. Upgrade the MicroLogix 1400 firmware to FRN 12 or higher.
2. Because of limitations in the MicroLogix 1100 platform, none of the firmware updates will be able to fix this issue, so users should use the following techniques to help reduce the likelihood of compromise.
3. Where possible, disable the Web server and change all default Administrator and Guest passwords.

4. If Web server functionality is needed, then Rockwell recommends upgrading the product's firmware to the most current version to have the newest enhanced protections available such as:
   a. When a controller receives two consecutive invalid authentication requests from an HTTP client, the controller resets the Authentication Counter after 60 minutes.
   b. When a controller receives 10 invalid authentication requests from any HTTP client, it will not accept any valid or invalid authentication packets until a 24-hour HTTP Server Lock Timer timeout.
5. If Web server functionality is needed, Rockwell also recommends configuring user accounts to have READ only access to the product so those accounts cannot be used to make configuration changes.

In addition to the above, Rockwell recommends concerned customers remain vigilant and continue to follow security strategies that help reduce risk and enhance overall control system security. Where possible, they suggest you apply multiple recommendations and complement this list with your own best-practices:

1. Employ layered security and defense-in-depth methods 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.
2. Restrict physical and electronic access to automation products, networks, and systems to only those individuals authorized to be in contact with control system equipment.
3. Employ firewalls with ingress/egress filtering, intrusion detection/prevention systems, and validate all configurations. Evaluate firewall configurations to ensure other appropriate inbound and outbound traffic is blocked.
4. Use up-to-date end-point protection software (e.g., antivirus/antimalware software) on all PC-based assets.
5. Make sure that software and control system device firmware is patched to current releases.
6. Periodically change passwords in control system components and infrastructure devices.
7. Where applicable, set the controller key-switch/mode-switch to RUN mode.

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

- Minimize network exposure for all control system devices. Critical devices should not directly face 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 VPN is only as secure as the connected devices.

ICS-CERT also provides a section for control systems security recommended practices on the US-CERT Web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[z] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01A—Targeted Cyber Intrusion Detection and Mitigation Strategies,[aa] that is available for download from the ICS-CERT Web page (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.

ICS-CERT CONTACT

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

Email: ics-cert@hq.dhs.gov
Toll Free: 1-877-776-7585

For industrial control systems security information and incident reporting: www.ics-cert.org

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/.

[z] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices html, Web site last accessed January 11, 2013.

[aa] Targeted Cyber Intrusion Detection and Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web site last accessed January 11, 2013.

DOCUMENT FAQ

What is an ICS-CERT Advisory? An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.

When is vulnerability attribution provided to researchers? Attribution for vulnerability discovery is always provided to the vulnerability reporter unless the reporter notifies ICS-CERT that they wish to remain anonymous. ICS-CERT encourages researchers to coordinate vulnerability details before public release. The public release of vulnerability details prior to the development of proper mitigations may put industrial control systems and the public at avoidable risk.