ID: PN1633 | Access Levels: Everyone

Remote Code Execution and Denial-of-Service Vulnerabilities in Select Communication Modules

Document ID	PN1633
Published Date	08/02/2023

Summary

Remote Code Execution and Denial-of-Service Vulnerabilities in Select Communication Modules

Revision History

Revision Number

1.0

Revision History

Version 1.0 – July 12, 2023

Executive Summary

Rockwell Automation, in coordination with the U.S. government, has analyzed a novel exploit capability attributed to Advance Persistent Threat (APT) actors affecting select communication modules. We are not aware of current exploitation leveraging this capability, and intended victimization remains unclear. Previous threat actors cyberactivity involving industrial systems suggests a high likelihood that these capabilities were developed with an intent to target critical infrastructure and that

victim scope could include international customers. Threat activity is subject to change and customers using affected products could face serious risk if exposed.

Rockwell Automation has provided patches for all affected products, including hardware series that were out of support. Detection rules have also been provided.

Exploitation of these vulnerabilities could allow malicious actors to gain remote access of the running memory of the module and perform malicious activity, such as manipulating the module's firmware, inserting new functionality into the module, wiping the module's memory, falsifying traffic to/from the module, establishing persistence on the module, and potentially affect the underlying industrial process. This could result in destructive actions where vulnerable modules are installed, including critical infrastructure.

Customers using the affected products are strongly encouraged to evaluate and implement the mitigations provided below. Additional details relating to the discovered vulnerabilities, including the products in scope, impact, and recommended countermeasures, are provided below.

Affected Products

Catalog	Series	Versions
1756-EN2T 1756-EN2TK 1756-EN2TXT	A,B,C	<=5.008 & 5.028
	D	<=11.003
1756-EN2TP 1756-EN2TPK 1756-EN2TPXT	A	<=11.003
1756-EN2TR 1756-EN2TRK 1756-EN2TRXT	A, B	<=5.008 & 5.028
	C	<=11.003
1756-EN2F 1756-EN2FK	A, B	<=5.008 & 5.028
	C	<=11.003
1756-EN3TR 1756-EN3TRK	A	<=5.008 & 5.028
	B	<=11.003

1756-EN4TR 1756-EN4TRK 1756-EN4TRXT	A	<=5.001

Vulnerability Details

CVE-2023-3595

Where this vulnerability exists in the 1756 EN2* and 1756 EN3* products, it could allow a malicious user to perform remote code execution with persistence on the target system through maliciously crafted CIP messages. This includes the ability to modify, deny, and exfiltrate data passing through the device.

```
CVSS score: 9.8/10 (Critical)
CVSS vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U
/C:H/I:H/A:H
CWE-787: Out-of-bounds Write
```


CVE-2023-3596

Where this vulnerability exists in the 1756-EN4* products, it could allow a malicious user to cause a denial of service by asserting the target system through maliciously crafted CIP messages.

```
CVSS Score: 7.5/10 (High)
CVSS vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U
/C:N/I:N/A:H
CWE-787: Out-of-bounds Write
```

Risk Mitigation & User Action

These vulnerabilities can be addressed by performing a standard firmware update. Customers are strongly encouraged to implement the risk mitigations provided below and to the extent possible, to combine these with the QA43240 - Recommended Security Guidelines from Rockwell Automation to employ multiple strategies simultaneously.

Catalog	Series	Affected Versions	Remediations
1756-EN2T 1756-EN2TK 1756-EN2TXT	A,B,C	<=5.008 & 5.028	• Update to 5.029 or later for signed versions (**recommended). • Update to 5.009 for unsigned versions.
	D	<=11.003	Update to 11.004 or later
1756-EN2TP 1756-EN2TPK 1756-EN2TPXT	A	<=11.003	Update to 11.004 or later
1756-EN2TR 1756-EN2TRK 1756-EN2TRXT	A, B	<=5.008 & 5.028	• Update to 5.029 or later for signed versions (**recommended). • Update to 5.009 for unsigned versions.
	C	<=11.003	Update to 11.004 or later
1756-EN2F 1756-EN2FK	A, B	<=5.008 & 5.028	• Update to 5.029 or later for signed versions (**recommended). • Update to 5.009 for unsigned versions.
	C	<=11.003	Update to 11.004 or later
1756-EN3TR 1756-EN3TRK	A	<=5.008 & 5.028	• Update to 5.029 or later for signed versions (**recommended). • Update to 5.009 for unsigned versions.
	B	<=11.003	Update to 11.004 or later
1756-EN4TR 1756-EN4TRK 1756-EN4TRXT	A	<=5.001	Update to 5.002 or later

** Rockwell Automation strongly recommends updating to signed firmware if possible. Once the module is updated to signed firmware (example 5.008 to 5.029), it is not possible to revert to unsigned firmware versions.

Mitigations

Organizations should take the following actions to further secure ControlLogix communications modules from exploitation.

- **Update firmware.** Update EN2* ControlLogix communications modules to firmware revision 11.004 and update EN4* ControlLogix communications modules to firmware revision 5.002.

- **Properly segment networks.** Given a cyber actor would require network connectivity to the communication module to exploit the vulnerability, organizations should ensure ICS/SCADA networks are properly segmented within the process structure as well as from the Internet and other non-essential networks.
- **Implement detection signatures.** Use appended Snort signatures to monitor and detect anomalous Common Industrial Protocol (CIP) packets to Rockwell Automation devices.

Additionally, organizations should increase protections of ICS/SCADA networks by implementing at least the following mitigations:

- Regularly back up devices to allow for reversion to a clean copy of firmware or a working project;
- disable unused CIP objects on communications modules, such as unused CIP Email and Socket Objects;
- block all traffic to CIP-enabled devices from outside the ICS/SCADA network using available security products; and
- monitor CIP traffic for unexpected content or unusual packets lengths.

Potential Indicators of Compromise

System owners should ensure ICS/SCADA networks are baselined and regularly monitored for deviations in network activity. Specifically, systems owners can look for the following potential IOCs (Indicators of Compromise) for ControlLogix communications modules:

- Unknown scanning on a network for Common Industrial Protocol (CIP)-enabled devices.
- Unexpected or out-of-specification CIP packets to CIP objects implemented in ControlLogix communications modules, including the Email Object and non-public vendor-specified objects.
- Arbitrary writes to communication module memory or firmware.
- Unexpected firmware updates.
- Unexpected disabling of secure boot options.
- Uncommon firmware file names.

Detection Rules

The following Snort rules are intended to be run on a computer with network visibility of a ControlLogix communications module and can be used to detect traffic to a ControlLogix communications module that does not conform to the CIP specification as provided by ODVA (Open DeviceNet Vendors Association). While both the CIP Email and Socket Objects are capable of communicating over a network, they are intended to communicate over the backplane of a ControlLogix PLC (Programmable Logic Controller) and therefore should not be seen over the network. However, it is possible that site engineers could configure a communications module such that there is legitimate network traffic to and from CIP Email and Socket Objects, potentially resulting in false positives.

Snort 2 Rules and Snort 3 Rules are both attached below.

References

- CVE-2023-3595 JSON
- CVE-2023-3596 JSON

Attachments

CVE-2023-3595 Snort 2.rules

File

File

CVE-2023-3595 Snort 3.rules

POSSIBILITY OF SUCH DAMAGES.

ROCKWELL AUTOMATION DISCLAIMS ALL WARRANTIES WHETHER EXPRESSED OR IMPLIED IN RESPECT OF THE INFORMATION (INCLUDING SOFTWARE) PROVIDED HEREBY, INCLUDING THE IMPLIED WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, AND NON-INFRINGEMENT. Note that certain jurisdictions do not countenance the exclusion of implied warranties; thus, this disclaimer may not apply to you.

www.rockwellautomation.com