ID: PN1550 | Access Levels: Everyone

# CVE-2021-22681: Authentication Bypass Vulnerability Found in Logix Controllers



| | |
|---|---|
| Document ID | PN1550 |
| Published Date | 03/05/2021 |

## Summary

CVE-2021-22681: Authentication Bypass Vulnerability Found in Logix Controllers

## Revision History

### Revision Number

1.0

### Revision History

Version 1.0 - February 25, 2021. Initial Release.

Top

## Revision History

## Revision Number

1.2

## Revision History

Version 1.2 - March 5, 2021. Updated for clarity.

## Executive Summary

Researchers found that our Studio 5000 Logix Designer® software may allow a key to be discovered. This key is used to verify Logix controllers are communicating with Rockwell Automation design software. If successfully exploited, this vulnerability could allow an unauthorized application to connect with Logix controllers. To leverage this vulnerability, an unauthorized user would require network access to the controller.

FactoryTalk® Security provides user authentication and authorization for a particular set of actions within RSLogix® 5000 and Studio 5000®. Once the application is authorized to open and connect to the controller within RSLogix 5000 or Studio 5000 this verification mechanism, referenced above, is leveraged to establish the connection to the controller. For customers concerned with user access control and who have deployed FactoryTalk Security, this vulnerability may allow an attacker to bypass the protections provided by FactoryTalk Security.

This vulnerability was independently co-discovered by Lab of Information Systems Security Assurance (Eunseon Jeong, Youngho An, Junyoung Park, Insu Oh, Kangbin Yim) of Soonchunhyang University, Kaspersky, and by Claroty, a cybersecurity technology vendor and partner of Rockwell Automation.

A **Rockwell Automation Internal Only** FAQ Document has been posted to Seismic.

## Affected Products

**Software:**

RSLogix 5000 software v16-20, Studio 5000 Logix Designer v21 and later, and corresponding Logix controllers running these versions.

Top

FactoryTalk Security, part of the FactoryTalk Services Platform, if configured and deployed v2.10 and later.

**Controllers:**

1768 CompactLogix™
1769 CompactLogix
CompactLogix 5370
CompactLogix 5380
CompactLogix 5480
ControlLogix 5550
ControlLogix® 5560
ControlLogix 5570
ControlLogix 5580
DriveLogix™ 5730
FlexLogix™ 1794-L34
Compact GuardLogix® 5370
Compact GuardLogix 5380
Guardlogix 5560
GuardLogix 5570
GuardLogix 5580
SoftLogix™ 5800

## Vulnerability Details

### CVE-2021-22681: Private Key Extraction

Studio 5000 Logix Designer uses a key to verify Logix controllers are communicating with Rockwell Automation products. If successfully exploited, this vulnerability could allow a remote, unauthenticated attacker to bypass a verification mechanism and authenticate with Logix controllers. If exploited, this vulnerability could enable an unauthorized third-party tool to make changes to the controller configuration and/or application code.

CVSS v3.1 Base Score: 10.0/CRITICAL
CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

## Risk Mitigation & User Action

Top

Customers using the affected products are directed towards risk mitigation and are encouraged, when possible, to combine this guidance with the general security guidelines for a comprehensive defense-in-depth strategy.

Rockwell Automation has determined that this vulnerability cannot be mitigated with a patch. Rockwell Automation encourages customers to implement the mitigation strategies outlined in this disclosure.

A comprehensive defense-in-depth strategy can reduce the risk of this vulnerability. To leverage this vulnerability, an unauthorized user requires network access to the controller. Customers should confirm that they are employing proper networking segmentation and security controls. Including, but not limited to:

- Minimizing network exposure for all control system devices and/or systems and confirm that they are not accessible from the Internet.
- Locating control system networks and devices behind firewalls and isolating them from the enterprise/business network.
- Restricting or blocking traffic on TCP 44818 from outside of the industrial control system network zone. For more information on the TCP/UDP ports used by Rockwell Automation products, see BF7490.
- 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. VPN is only as secure as the connected devices.

Customers can refer to the Converged Plantwide Ethernet (CPwE) Design and Implementation Guide for best practices for deploying network segmentation and broader defense in depth strategies. Customers can also refer to the Rockwell Automation System Security Design Guidelines on how to use Rockwell Automation products to improve the security of their industrial automation systems.

CIP Security mitigates this vulnerability as it provides the ability to deploy TLS and DTLS based secure communications to supported products. CIP Security is an enhancement to

the ODVA EtherNet/IP industrial communication standard and directly addresses the vulnerability noted in this disclosure. CIP Security allows for users to leverage and manage certificates and/or pre-shared keys and does not make use of any hardcoded keys.

Customers requiring setup or deployment guidance for CIP Security protocol should refer to the CIP Security deployment refence guide for more information.

For additional details and further mitigation options, please see the table below.

| Product Family and Version | Additional Risk Mitigation and Recommended User Actions |
|---|---|
| ControlLogix 5580 v32 or later. | • Put controller mode switch to "Run" mode.<br>If the above cannot be deployed, the followings mitigations are recommended:<br>• Deploy CIP Security for Logix Designer application connections through the front port. CIP Security prevents unauthorized connections when deployed properly.<br>• If not using the front port, use a 1756-EN4TR ControlLogix EtherNet/IP™ module and deploy CIP Security. The 1756-EN4TR supports CIP Security, which prevents unauthorized connections when properly deployed. |
| ControlLogix 5580 v31 | • Put the controller mode switch to “Run” mode.<br>If the above cannot be deployed, the following mitigations are recommended:<br>• Apply v32 or later and follow mitigations actions outlined above.<br>• If unable to apply a newer version, use a 1756-EN4TR ControlLogix EtherNet/IP module and deploy CIP Security. The 1756-EN4TR supports CIP Security, which helps prevent unauthorized connections when properly deployed. |

Top

| Product Family and Version | Additional Risk Mitigation and Recommended User Actions |
|---|---|
| ControlLogix 5570 v31 or later. | • Put the controller mode switch to “Run” mode.<br>If the above cannot be deployed, the following mitigations are recommended:<br>• Use a 1756-EN4TR ControlLogix EtherNet/IP Module and deploy CIP Security. The 1756-EN4TR supports CIP Security, which helps prevent unauthorized connections when properly deployed. |
| ControlLogix 5580 v28-v30<br>ControlLogix 5570 v18 or later.<br>ControlLogix 5560 v16 or later.<br>ControlLogix 5550 v16.<br>GuardLogix 5580 v31 or later.<br>GuardLogix 5570 v20 or later.<br>GuardLogix 5560 v16 or later.<br>1768 CompactLogix v16 or later.<br>1769 CompactLogix v16 or later.<br>CompactLogix 5370 v20 or later.<br>CompactLogix 5380 v28 or later.<br>CompactLogix 5480 v32 or later.<br>Compact GuardLogix 5370 v28 or later.<br>Compact GuardLogix 5380 v31 or later.<br>FlexLogix 1794-L34 v16.<br>DriveLogix 5370 v16 or later. | • Put the controller mode switch to “Run” mode. |
| SoftLogix 5800 | • No additional mitigation available. Follow the Converged Plantwide Ethernet (CPwE) Design and Implementation Guide. |

## Detection Strategies:

In addition, customers can continue to use the methods below to detect changes to configuration or application files:

Top

- Monitor controller change log for any unexpected modifications or anomalous activity.
- If using v17 or later, utilize the Controller Log feature.
- If using v20 or later, utilize Change Detection in the Logix Designer Application.
- If available, use the functionality in FactoryTalk® AssetCentre software to detect changes.

## General Security Guidelines

### Network-based Vulnerability Mitigations for Embedded Products

- Consult the product documentation for specific features, such as a hardware Mode Switch setting, which may be used to block unauthorized changes, etc.

### Social Engineering Mitigation Strategies

- Do not click on or open URL links from untrusted sources.
- Employ training and awareness programs to educate users on the warning signs of a phishing or social engineering attack.

### General Mitigations

- Use trusted software, software patches, antivirus/antimalware programs and interact only with trusted web sites and attachments.
- Minimize network exposure for all control system devices and/or systems and confirm that they are not accessible from the Internet. For further information about the risks of unprotected Internet accessible control systems, please see Knowledgebase Article PN715.
- Locate control system networks and devices behind firewalls and isolate them from the business network.

For further information on the Vulnerability Handling Process for Rockwell Automation, please refer to our Product Security Incident Response FAQ document.

Refer to our Industrial Network Architectures Page for comprehensive information about implementing validated architectures designed to complement security solutions.

Top

See the Network Services Overview Page for information on network and security services for Rockwell Automation to enable assessment, design, implementation and management of validated, secure network architectures.

We also recommend that concerned customers continue to monitor this advisory by subscribing to PSA/PN/Security Notifications. This can be done by updating settings in Account Overview within the KnoweldgeBase.

Rockwell Automation remains committed to making security enhancements to our systems in the future. For more information and for assistance with assessing the state of security of your existing control system, including improving your system-level security when using Rockwell Automation and other vendor controls products, you can visit the Rockwell Automation Security Solutions web site.

**Requests for additional information can be sent to the RASecure Inbox (rasecure@ra.rockwell.com).**

**ADDITIONAL LINKS**

- PN1354 - Industrial Security Advisory Index
- Industrial Firewalls within a CPwE Architecture
- Deploying Industrial Firewalls within a CPwE Architecture Design and Implementation Guide
- ICSA-21-056-03

Anomaly ID

PSORAR-5869

## Recently Viewed

Top

Functions of Auxiliary Contacts and Adding Contacts to Bulletin 505 / 520 Starters

Wiring Diagram for Bulletin 520E Starter using E1 Plus solid-state Overload Relays



**www.rockwellautomation.com**



Top