CYBERTROL ENGINEERING
CONTROL & INFORMATION SYSTEM INTEGRATION
EXCELLENCE · INTEGRITY · ACHIEVMENT · SAFETY

Security Technote and Recommended Action

CVE-2021-22681 Rockwell Vulnerability

There is a recent vulnerability released in Rockwell Automation software where the authentication mechanism for communication to PLC's has been compromised.

Rockwell controllers use a security key to validate that PLC's are connecting with Rockwell Automation software. There is a vulnerability in RSLogix (v16-20) / Studio 5000 (v21+) where this key has been compromised, allowing any third-party tool to alter the controller's configuration.

A CVSS v3 base score of 10.0 has been calculated (maximum). This is a very severe vulnerability if exploited could impact production wherever vulnerable PLCs are used.

The following PLC's are affected:

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

Proper network segmentation and security controls should be implemented to reduce the exposure to these devices.

Cybertrol recommends the following should be considered as part of a defense in depth strategy.

- Limit access to PLC's from dedicated and monitored programming servers.
- Limit access to programming servers with multi-factor authentication through a DMZ architecture.
- Ensure equipment has vulnerabilities patched to reduce the chance of running code exploiting this vulnerability. (Especially firewalls and servers, and DMZ infrastructure.)
- Implement a DMZ architecture without direct access to production equipment from above the DMZ.
    - Ensure production systems are not accessible from the internet.
    - Locate production networks behind a firewall to limit access from the DMZ and business networks.
    - Utilize secure methods of remote access when required.
    - Ensure methods of remote access is up to date to minimize any potential vulnerabilities.
- Put controller's mode switch into 'Run' - only place in 'Rem' for the time it takes to implement changes. Immediately switch back to 'Run' after any changes.
- Implement CIP security with the front ethernet ports on controllers, or with a 1756-EN4TR.
- Monitor the controller change log for any unexpected modifications or activity.
- Utilize change detection in Logix Designer.
- Use AssetCentre to detect changes where available.
- Monitor PLC traffic to identify any unexpected devices communicating with the controller.

For more information, please contact Cybertrol Engineering https://www.cybertrol.com and visit the Cybersecurity and Infrastructure Security Agency page on this vulnerability: https://us-cert.cisa.gov/ics/advisories/icsa-21-056-03