Allen Bradley Micrologix 1100 – Known vulnerabilities

Overview

The Allen-Bradley MicroLogix 1100 is a programmable logic controller (PLC) produced by Rockwell Automation. The following will list the known vulnerabilities of the device. The impact of such vulnerabilities range from being able to reset the device all the way to gaining access and performing unintended functions.

Known Vulnerabilities

1. **Cleartext transmission of sensitive information** - User credentials are sent to web server in clear text which could be intercepted / viewed, resulting in unwanted gaining administrative privilege (such as forcing device into state requiring factory reset)
2. **Stack-Based Buffer Overflow** – This vulnerability performed by a user to pass data that can overflow a buffer and provide an attacker the ability to potentially execute arbitrary code.
3. **Improper restriction of operations within the bounds of a memory buffer** – A specific web request may allow attacker to crash device which would require the device to be reset / power-cycled
4. **Unrestricted upload of file with dangerous type** – Remote attacker could redirect web content to the device's 'web frame' allowing for remote file inclusion which could be malware, malicious code, etc.
5. **Cross-site scripting** – An attacker could inject malicious JavaScript into device's web server which would then be executed on client side's web browser resulting in possible malicious activity
6. **SQL- Injection** – Specific malicious input could result in deleting users, adding users, escalating privileges, etc.

Source

All information was found on the ICS-CERT website, specifically: ttps://ics-cert.us-cert.gov/advisories/ICSA-15-300-03A