WEDNESDAY, MARCH 28, 2018

Vulnerability Spotlight: Multiple Vulnerabilities in Allen Bradley MicroLogix 1400 Series Devices

These vulnerabilities were discovered by Jared Rittle and Patrick DeSantis of Cisco Talos.

SUMMARY

Rockwell Automation Allen-Bradley MicroLogix 1400 Programmable Logic Controllers (PLCs) are marketed for use in a variety of different Industrial Control System (ICS) applications and processes. As such, these devices are often relied upon for the performance of critical process control functions in many different critical infrastructure sectors. Previously, Cisco Talos released details regarding a vulnerability that was present in these devices. Cisco Talos continued analysis of these devices and discovered additional vulnerabilities that could be leveraged to modify device configuration and ladder logic, write modified program data into the device's memory module, erase program data from the device's memory module, or conduct Denial of Service (DoS) attacks against affected devices. Depending on the affected PLCs within an industrial control process, this could result in significant damages.

VULNERABILITY DETAILS

Allen-Bradley MicroLogix 1400 Series B Ethernet Card Malformed Packet Denial of Service Vulnerability (TALOS-2017-0440 / CVE-2017-12088)

This vulnerability would allow an unauthenticated attacker to send a specially crafted packet causing affected devices to power cycle and enter into a fault state. This results in the deletion of ladder logic previously stored on the devices. It is important to note that this vulnerability is not leveraged using the EtherNet/IP protocol, so simply disabling EtherNet/IP using RSLogix will not provide effective mitigation. For complete details regarding this vulnerability, please see the advisory here.

Allen-Bradley MicroLogix 1400 Series B Ladder Logic Program Download Device Fault Denial of Service Vulnerability (TALOS-2017-0441 / CVE-2017-12089)

This vulnerability would allow an unauthenticated attacker to send a specially crafted packet causing a denial of service condition. The vulnerability lies in the program download functionality of affected

devices, allowing an attacker to force the devices into a fault condition by sending an 'Execute Command List' (CMD 0x0F, FNC 0x88) packet without following it up with a 'Download Complete' (CMD 0x0F, FNC 0x52). When this occurs, the device processes this as a failure condition and enters the non-user fault mode, causing it to cease normal operations and delete any stored logic. For complete details regarding this vulnerability, please see the advisory here.

Allen-Bradley MicroLogix 1400 Series B SNMP-Set Processing Incorrect Behavior Order Denial of Service Vulnerability (TALOS-2017-0442 / CVE-2017-12090)

This vulnerability is related to how the devices process 'snmp-set' commands received during a firmware update and could allow an authenticated attacker to cause a Denial of Service condition to occur on affected devices. By sending a specially crafted 'snmp-set' command without sending the subsequent 'snmp-set' commands that are normally associated with the final command sent during the firmware update process, the attacker could force the device to power cycle making it unavailable for the duration of the reboot process. While this vulnerability does require valid SNMP credentials, hard coded SNMP credentials (as documented in the advisory here) could be leveraged to obtain this level of access to affected devices. For complete details regarding this vulnerability, please see the advisory here.

Allen-Bradley MicroLogix 1400 Series B Unauthenticated Data/Program/Function File Improper Access Control Vulnerability (TALOS-2017-0443 / CVE-2017-14462 - CVE-2017-14473)

This vulnerability is related to improper file access controls on affected devices. This vulnerability allows an unauthenticated attacker to perform read and write operations on files stored on the devices. This could be used to retrieve sensitive information from affected devices including the device master password, modify device settings or ladder logic, or cause the device to enter a fault condition causing a Denial of Service condition. For complete details regarding this vulnerability, please see the advisory here.

Allen-Bradley MicroLogix 1400 Series B Memory Module Store Program File Write Vulnerability (TALOS-2017-0444 / CVE-2017-12092)

This vulnerability allows an unauthenticated remote attacker to write the online program to the installed memory module on affected devices. An attacker could use this to store program modifications that are unable to take effect until a device power cycle. An attacker could subsequently use the newly stored program in conjunction with the 'Load Memory Module On Memory Error' setting to modify system settings, resulting in changes to enabled services.For complete details regarding this vulnerability, please see the advisory here.

Allen-Bradley MicroLogix 1400 Series B PLC Session Communication Insufficient Resource Pool Denial of Service Vulnerability (TALOS-2017-0445 / CVE-2017-12093)

This vulnerability is present in the session connection functionality on affected devices. By default, these devices support a maximum of ten simultaneous connections. Once this maximum has been reached, the device will terminate the oldest connection to make room in the connection pool for new connections that are established with the device. An unauthenticated attacker can send several 'Register Session' packets over a period of time to force legitimate connections to be terminated and prevent the establishment of additional legitimate connections to affected devices. For complete details regarding this vulnerability, please see the advisory here.

AFFECTED VERSIONS

Cisco Talos has tested and confirmed that the following versions are affected by these vulnerabilities:

Allen-Bradley Micrologix 1400 Series B FRN 21.003
Allen-Bradley Micrologix 1400 Series B FRN 21.002
Allen-Bradley Micrologix 1400 Series B FRN 21.0
Allen-Bradley Micrologix 1400 Series B FRN 15

CONCLUSION

As these devices are often deployed to support critical industrial control processes, it is recommended that organizations making use of affected devices upgrade to the latest version of firmware so that devices are no longer affected by these vulnerabilities. An advisory related to these vulnerabilities has been published, which can be found here.

COVERAGE

The following Snort SIDs have been added to detect attempts to exploit these vulnerabilities:

Snort Rules: 44419 - 44429

POSTED BY EDMUND BRUMAGHIN AT 3:59 PM
LABELS: ICS, PLC, ROCKWELL AUTOMATION, VULNERABILITY RESEARCH

SHARE THIS POST