

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>

DATE(S) ISSUED:

01/27/2016

SUBJECT:

A Vulnerability in Rockwell Automation MicroLogix 1100 PLC Systems Could Allow Remote Code Execution

OVERVIEW:

A vulnerability has been identified in the Rockwell Automation MicroLogix 1100 PLC Systems that could allow remote code execution on the affected device. The affected Programmable Logic Controller (PLC) is used across several sectors, including chemical, critical manufacturing, food and agriculture, water and wastewater systems. Successful exploitation of this vulnerability could allow an attacker to perform remote code execution on the affected device.

THREAT INTELLIGENCE:

There are currently no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:

- 1763-L16AWA, Series B, Version 15.000 and prior versions
- 1763-L16BBB, Series B, Version 15.000 and prior versions
- 1763-L16BWA, Series B, Version 15.000 and prior versions
- 1763-L16DWD, Series B, Version 15.000 and prior versions
- 1763-L16AWA, Series A, Version 15.000 and prior versions
- 1763-L16BBB, Series A, Version 15.000 and prior versions
- 1763-L16DWD, Series A, Version 15.000 and prior versions

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: N/A

TECHNICAL SUMMARY:

A stack-based buffer overflow vulnerability has been discovered in Rockwell Automation MicroLogix 1100 PLC Systems that could allow remote code execution on the affected device. This vulnerability can be exploited when the device receives a malicious web based request. CVE-2016-0868 has been assigned to this vulnerability.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate updates provided by Rockwell Automation to vulnerable PLCs, immediately after appropriate testing.
- Note that Rockwell Automation has not provided an update for MicroLogix 1100 controller, hardware Series A.
- Limit access to the device to authorized hosts.
- If appropriate, disable the web server on the MicroLogix 1100, as it is enabled by default.
- Review log files to determine if the identified vulnerability was exploited, and remediate per your security policy and procedures.

REFERENCES:

ICS-CERT:

<https://ics-cert.us-cert.gov/advisories/ICSA-16-026-02>

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>