



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

August 12, 2016

The following cyber advisory was issued by the State of Alaska and was 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.

ADVISORY NUMBER:

SA2016-121

DATE(S) ISSUED:

08/12/2016

SUBJECT:

A Vulnerability in Rockwell Automation MicroLogix 1400 PLC Systems Could Allow for Unauthorized Remote Access

OVERVIEW:

A vulnerability has been discovered in the Rockwell Automation MicroLogix 1400 Programmable Logic Controller (PLC) Systems that could allow for unauthorized remote access. These affected Industrial Control System (ICS) products are used across several sectors, including Chemical, Critical Manufacturing, Food and Agriculture, Water and Wastewater Systems and others. 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:

- 1766-L32BWA
- 1766-L32AWA
- 1766-L32BXB
- 1766-L32BWAA
- 1766-L32AWAA
- 1766-L32BXBA

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 vulnerability has been discovered in Rockwell Automation MicroLogix 1400 PLC that could allow for undocumented and privileged Simple Network Management Protocol (SNMP) access via a community string. This vulnerability can be exploited when SNMP is open on the network as it is by default to allow for firmware updates. (CVE-2016-5646)

RECOMMENDATIONS:

Rockwell Automation has not provided an update for MicroLogix 1400 controller. Due to the nature of the process, this capability cannot be removed from the PLCs and will not be patched. We recommend one of the following mitigation actions be applied:

- Limit access to the device to authorized hosts. Where possible, locate the devices behind firewalls and if remote access is required, use secure methods such as virtual private networks (VPN).
- Utilize the product's "RUN" keyswitch setting to prevent unauthorized and undesired firmware update operations and other disruptive configuration changes.
- If appropriate, disable SNMP on the MicroLogix 1400.
 - **Note:** It will be necessary to re-enable SNMP to update firmware on this product. After the upgrade is complete, disable the SNMP service once again.
- Review log files to determine if the identified vulnerability was exploited, and remediate per your security policy and procedures.
- **Note:** Changing the SNMP community strings is not an effective mitigation.

REFERENCES:

ICS-CERT:

<https://ics-cert.us-cert.gov/advisories/ICSA-16-224-01>

CVE:

<http://cwe.mitre.org/data/definitions/250.html>