



**ICS-CERT**

**INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM**

# ICS-CERT ADVISORY

ICSA-10-322-02A— AUTOMATED SOLUTIONS OPC SERVER VULNERABILITY

## **UPDATE A**

January 21, 2011

### OVERVIEW

The ICS-CERT has received a report from independent security researcher Jeremy Brown that reveals a heap corruption vulnerability in the Automated Solutions Modbus/TCP Master OPC server. Automated Solutions has confirmed that their most recent patch mitigates the vulnerability for Version 3.0.0. ICS-CERT has verified that the software update resolves the vulnerability identified by the researcher.

#### **----- Begin Update A-----**

The vulnerability could be exploited by creating a Modbus/TCP Slave application that generates non-compliant Modbus/TCP reply packets. Successful exploitation would likely not allow arbitrary code execution; however, an exploit could possibly corrupt the OPC server memory.

#### **----- End Update A-----**

### AFFECTED PRODUCTS

This vulnerability affects the Automated Solutions Modbus/TCP Master OPC Server product (Version 3.0.0) and all previous versions.

#### **----- Begin Update A-----**

According to Automated Solutions, no other products share the OPC Server code base.

#### **----- End Update A-----**

### IMPACT

Automated Solutions' customers include a large cross section of ICS vendors, including Supervisory Control and Data Acquisition (SCADA) vendors who also supply OPC server products to end users and integrators.

While an exploit is unlikely to allow arbitrary code execution, the impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their environment, architecture, and product implementation.



## ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

### BACKGROUND

Automated Solutions supplies Modbus/TCP OPC Data Access OPC servers in an original equipment manufacturer (OEM) version and a stand-alone version. This advisory currently applies only to the stand-alone version.

### VULNERABILITY CHARACTERIZATION

----- **Begin Update A**-----

### VULNERABILITY OVERVIEW

The vulnerability is a heap-based buffer overflow that can be exploited by creating or compromising a Modbus/TCP Slave to generate non-compliant Modbus/TCP header length values. It is unlikely that arbitrary code execution is possible; however, it is possible to corrupt the OPC server memory. That memory corruption could result in the OPC server failing, leading to corrupted or lost data.

### VULNERABILITY DETAILS

#### EXPLOITABILITY

The vulnerability allows an attacker to write an arbitrary number of double words or DWORDs onto the heap; however, it is not possible to control the content of the DWORDs. Therefore, it is unlikely the vulnerability could allow arbitrary code execution. However, it is possible to write data past the memory allocated in the heap, thus overwriting memory that is available to, and potentially used by, the OPC server process.

It is important to note that, to exploit this vulnerability, one or both of the following conditions must be met:

1. The Modbus/TCP Slave device is not Modbus/TCP compliant with regard to Modbus/TCP header length field.
2. An attacker must be capable of modifying the slave's operating program so that it sends a reply packet with an invalid Modbus/TCP header length field to compromise the Modbus/TCP Slave device.

#### EXISTENCE OF EXPLOIT

No exploit code is known to exist beyond the test code developed by the researcher, which was also used by ICS-CERT to validate the vulnerability.

#### DIFFICULTY

An attacker with at least an intermediate skill level could create code to exploit this vulnerability.

----- **End Update A**-----



## ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

### MITIGATION

ICS-CERT recommends that users of the Automated Solutions Modbus/TCP Master OPC Server (stand-alone) take the following mitigation steps:

- Upgrade to the latest version and install the latest patch.  
Automated Solutions has developed a patch for the OPC Server (Version 3.0.0); ICS-CERT has verified that the software update resolves the vulnerability identified by the researcher. The patch is available at <http://automatedsolutions.com/demos/demoform.asp?code=17>.
- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet. Control system networks and remote devices should be located behind firewalls, and be isolated from the business network. If remote access is required, secure methods such as Virtual Private Networks (VPNs) should be utilized.

Owners and operators should exercise caution and consult their control systems vendor prior to making any changes. Proper impact analysis and testing should always be conducted prior to making any changes to control systems.

Organizations should follow their established internal procedures if any suspected malicious activity is observed and report their findings to ICS-CERT for tracking and correlation against other incidents. ICS-CERT reminds organizations that proper impact analysis and risk assessment should be performed prior to taking defensive measures.

The Control System Security Program also provides a recommended practices section for control systems on the US-CERT web site. Several recommended practices are available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*.<sup>1</sup>

### ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

E-mail: [ics-cert@dhs.gov](mailto:ics-cert@dhs.gov)

Toll free: 1-877-776-7585

For Control System Security Program Information and Incident Reporting: [www.ics-cert.org](http://www.ics-cert.org).

### DOCUMENT FAQ

**What is an ICS-CERT Advisory?** An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.

---

1. Control System Security Program (CSSP) Recommended Practices, [http://www.us-cert.gov/control\\_systems/practices/Recommended\\_Practices.html](http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html)