ICS-CERT ADVISORY

ICSA-11-018-01—AGG SCADA VIEWER OPC BUFFER OVERFLOW VULNERABILITY

January 24, 2011

OVERVIEW

The ICS-CERT has received a report from independent security researcher Steven James that a stack-based buffer overflow exists in the AGG Software OPC SCADA Viewer software. The vulnerability could allow arbitrary code execution. ICS-CERT has coordinated with AGG Software, which has developed a patch to address this vulnerability. The researcher has also verified that the patch resolves the issue.

AFFECTED PRODUCTS

This vulnerability affects all OPC SCADA Viewer versions prior to Version 1.5.2 (Build 110).

IMPACT

A successful exploit of this vulnerability could lead to arbitrary code execution. The exact 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.

BACKGROUND

AGG Software[a] is a North American company that produces data acquisition, data logging, and monitoring software for hardware interfaces. OPC SCADA Viewer is a tool that displays data received through the OPC interface.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

OPC SCADA Viewer is vulnerable to a stack-based buffer overflow. An attacker can craft a special configuration file that can allow arbitrary code execution when parsed by OPC SCADA Viewer.

a. AGG Software, http://www.aggsoft.com, web page accessed January 17, 2011.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is exploitable from the local machine.

EXISTENCE OF EXPLOIT

No publicly available exploit is known to exist.

DIFFICULTY

A moderate level of skill is needed to exploit this vulnerability.

MITIGATION

ICS-CERT recommends that users of OPC SCADA Viewer take the following mitigation steps:

- Update OPC SCADA Viewer to the latest version (1.5.2 (Build 110)) or install Update Version 1.5.2 build 110 to patch releases since Version 1.5.0. The latest version and update can be found on AGG's OPC SCADA Viewer download page:

  http://www.aggsoft.com/opc-scada/download.htm

- Do not open configuration files from an untrusted source.

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 website. Several recommended practices are available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*.[b]

b. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html.

ICS-CERT CONTACT

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

E-mail: ics-cert@dhs.gov
Toll free: 1-877-776-7585

For Control System Security Program Information and Incident Reporting: 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.