ICS-CERT ADVISORY

ICSA-10-264-01—SCADA ENGINE BACNET OPC CLIENT BUFFER OVERFLOW VULNERABILITY

September 21, 2010

OVERVIEW

A buffer overflow vulnerability has been reported[a] in SCADA Engine's BACnet OPC Client. Using a specially crafted malicious file, this vulnerability could allow an attacker to crash the application and execute arbitrary code. A software update is available that resolves this vulnerability.

ICS-CERT is aware that exploit code for this vulnerability is publicly available.[b] However, ICS-CERT has not received any reports of the vulnerability being exploited in the wild.

AFFECTED PRODUCTS

ICS-CERT has confirmed the vulnerability in Version 1.0.24. Older versions may also be affected.

SCADA Engine has released a software update, Version 1.0.25, which ICS-CERT has confirmed effectively mitigates the vulnerability.

IMPACT

User interaction is required to successfully exploit this vulnerability. If the vulnerability is exploited successfully, arbitrary execution of code is possible.

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

SCADA Engine's BACnet OPC client connects an OPC server to any BACnet compliant device. The client supports OPC Data Access Specification 1.0 and 2.0 and OPC Alarms and Events Specification 1.0. The Client supports the DS-RP-A, DS-RPM-A, DS-WP-A, DS-WPM-A, DS-COV-A, DS-COVU-A,

a.Secunia Advisory SA41466, http://secunia.com/advisories/41466/, website last accessed September 21, 2010
b. http://packetstormsecurity.org/1009-exploits/bacnet-overflow.py.txt, website last accessed September 21, 2010

AE-N-A, AE-ACK-A, AE-ASUM-A, AE-ESUM-A, DM-DDB-A and SCHED-A BACnet Interoperability Building Blocks (BIBBs).[c]

The BACnet OPC Client is supported on the following operating systems: Windows NT 4.0, Windows 2000, and Windows XP.

The BACnet protocol was developed by the American Society of Heating, Refrigerating, and Air-Conditioning Engineers (ASHRAE) and is generally used for building automation and control systems. Building automation products are used to control all aspects of a building, such as:

- Heating, cooling, and ventilation
- Chillers, boilers
- Air handling units
- Security, lighting
- Miscellaneous equipment.[d]

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

Security researcher Jeremy Brown discovered a stack-based buffer overflow in SCADA Engine's BACnet OPC Client. A boundary error exists in WTclient.dll when preparing a status log message. This can be exploited to create a buffer overflow when the client opens a specially crafted malicious file (e.g., *.csv file).

VULNERABILITY DETAILS

EXPLOITABILITY

Successful exploitation of this vulnerability results in arbitrary code execution potentially leading to a system compromise. A successful exploit requires that a user open a specially crafted file.

EXISTENCE OF EXPLOIT

Exploit code for this vulnerability is publicly available.[b]

DIFFICULTY

Social engineering is required to convince the user to open the malicious file. This increases the difficulty of a successful exploit.

c. BACnet OPC Client, http://www.scadaengine.com/software7.html, website last accessed September 21, 2010
d. BACnet Software for Building Automation, http://www.scadaengine.com, website last accessed September 21, 2010

MITIGATION

A software update is available and can be downloaded from the SCADA Engine download page.[e]

Until the update is applied, ICS-CERT recommends industrial control systems owners and operators take extreme caution when opening unexpected or untrusted files, especially *.csv files.

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 Systems 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.*[f]

In addition, ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks:

- Do not click web links or open unsolicited attachments in e-mail messages
- Refer to *Recognizing and Avoiding Email Scams*[g] for more information on avoiding e-mail scams
- Refer to *Avoiding Social Engineering and Phishing Attacks*[h] for more information on social engineering attacks.

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

e. SCADA Engine Download Page, http://www.scadaengine.com/downloads.html, website last accessed September 21, 2010
f. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed September 21, 2010
g. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf., website last accessed March 5, 2010
h. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed March 4, 2010