ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ALERT

ICS-ALERT-10-260-01 - SCADA ENGINE BACNET OPC CLIENT BUFFER OVERFLOW VULNERABILITY

September 17, 2010

ALERT

SUMMARY

ICS-CERT is aware of reports describing a vulnerability in SCADA Engine's BACnet OPC Client, which could be used for arbitrary code execution. The vulnerability is reportedly due to a boundary error in WTclient.dll when preparing a status log message. This can be exploited to create a stack-based buffer overflow when a user opens a specially crafted file (e.g., *.csv file). This vulnerability has been reported to be confirmed in Version 1.0.24. However, other versions may also be affected. ICS-CERT is in the process of confirming these reports with the vendor.

The BACnet protocol was developed by ASHARE and is generally used for Building Automation and Control systems. It has been implemented by many manufacturers of Building Automation products. The SCADA Engine BACnet OPC Client supports OPC Data Access Specification 1.0 and 2.0 and Event/Alarm Specification 1.0. Supported operating systems are Windows NT 4.0, Windows 2000, and Windows XP.

ICS-CERT is not currently aware of a workaround or patch for this vulnerability. ICS-CERT recommends industrial control systems owners and operators take extreme caution when opening unexpected or untrusted files, especially *.csv files. ICS-CERT is in the process of contacting the vendor and will provide updates as appropriate.

Please report any issues affecting control systems in critical infrastructure environments to ICS-CERT.

Other resources:

http://secunia.com/advisories/41466
http://www.bacnet.org/

ICS-CERT Operations Center
1-877-776-7585
www.ics-cert.org
ICS-CERT@DHS.GOV

What is an ICS-CERT Alert? An ICS-CERT Alert is intended to provide timely notification to critical infrastructure owners and operators concerning threats or activity with the potential to impact critical infrastructure computing networks.