ICS-CERT ADVISORY

ICSA-12-012-01**A**— OPEN AUTOMATION SOFTWARE OPC SYSTEMS.NET VULNERABILITY

UPDATE A

January 26, 2012

OVERVIEW

This Advisory is a follow-up to "ICS-ALERT-11-285-01—Open Automation Software OPC Systems.NET vulnerability" that was posted on the ICS-CERT website on October 12, 2011.

Independent researcher Luigi Auriemma publicly reported a malformed packet vulnerability in Open Automation Software's OPC Systems.NET along with proof-of-concept (PoC) exploit code. This public report was released without coordination with Open Automation Software, ICS-CERT, or any other coordinating entity known to ICS-CERT.

ICS-CERT has coordinated this vulnerability with Open Automation Software, and they have produced an update that resolves this vulnerability. Luigi Auriemma has tested the update and has confirmed that it resolves the vulnerability.

--------- Begin Update A Part 1 of 2 --------

On January 20, 2012, Digital Security Research Group publicly reported a buffer overflow vulnerability in a third-party ActiveX control in OPC Systems.NET. This public report was released without coordination with Open Automation Software, ICS-CERT, or any other coordinating entity known to ICS-CERT.

--------- End Update A Part 1 of 2 --------

AFFECTED PRODUCTS

All versions of OPC Sytems.NET prior to Version 5.0 are affected.

IMPACT

A malformed packet could be sent remotely to cause a denial of service.

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 control system environment, architecture, and product implementation.

BACKGROUND

Open Automation Software is a US-based company that provides .NET products for supervisory control and data acquisition (SCADA) and human-machine interfaces (HMI) applications.

According to Open Automation Software, OPC Systems.NET is an HMI application that is deployed across several sectors including manufacturing, information technology, energy, water and wastewater, defense, and others. Open Automation Software estimates that these products are used throughout the world with primary use in the United States.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

MALFORMED PACKET VULNERABILITY

The vulnerability is exploitable by sending a malformed .NET Remote Procedural Call (RPC) packet to cause a denial of service through Port 58723/TCP.

CVE-2011-4871[a] has been assigned to this vulnerability.

--------- Begin Update A Part 2 of 2 --------

BUFFER OVERFLOW VULNERABILITY

Third-party ActiveX component FlexGrid 7.1 is vulnerable to a buffer overflow attack.

CVE-2012-0227[b] has been assigned to this vulnerability.

--------- End Update A Part 2 of 2 --------

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities are remotely exploitable.

EXISTENCE OF EXPLOIT

Public exploits are known to target these vulnerabilities.

a. http://web nvd nist.gov/view/vuln/detail?vulnId=CVE-2011-4871, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.
b. http://web nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0227, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

DIFFICULTY

Crafting working exploits for these vulnerabilities requires moderate skill.

MITIGATION

Open Automation Software has released OPC Systems.NET Version 5.0[c] that resolves the reported vulnerabilities by removing the vulnerable component. Customers with vulnerable versions of Open Automation Software OPC Sytems.NET should deploy the update, which is available at: www.opcsystems.com/downloads.htm.

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet.
- Locate control system networks and remote devices behind firewalls with properly configured rules—particularly TCP Port 58723—and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

The Control Systems Security Program (CSSP) also provides a section for control systems security recommended practices on the CSSP web page. Several recommended practices are available for reading and download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*[d] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

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

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

c. Open Automation Software Releases OPC Systems.NET Version 5.0 with Enhanced Network Security, http://www.opcsystems.com/news/wcf.htm, website last accessed January 25, 2012.

d. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices html, website last accessed January 25, 2012.

e. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed January 25, 2012.

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 CSSP 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.

When is vulnerability attribution provided to researchers? Attribution for vulnerability discovery is always provided to the vulnerability reporter unless the reporter notifies ICS-CERT that they wish to remain anonymous. ICS-CERT encourages researchers to coordinate vulnerability details before public release. The public release of vulnerability details prior to the development of proper mitigations may put industrial control systems and the public at avoidable risk.

f. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014 html, website last accessed January 09, 2012.