ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-11-279-01—ADVANTECH OPC SERVER BUFFER OVERFLOW

November 04, 2011

OVERVIEW

ICS-CERT originally released Advisory ICSA-11-279-01P on the US-CERT secure Portal on October 06, 2011. This web page release was delayed to allow users time to download and install the update.

Security research and service institute Information and Communication Security Technology Center (ICST) has identified a buffer overflow vulnerability that affects multiple Advantech OPC (OLE for Process Control) Server products. This vulnerability may allow remote code execution and elevated user privileges.

Advantech has produced a new software version that mitigates this vulnerability. ICST has tested the new version and confirmed that it fully resolves this vulnerability.

AFFECTED PRODUCTS

The following versions of OPC Server are affected:

- Advantech ADAM OPC Server Versions prior to V3.01.012
- Advantech Modbus RTU OPC Server Versions prior to V3.01.010
- Advantech Modbus TCP OPC Server Versions prior to V3.01.010.

IMPACT

Impact to individual organizations depends on many operational factors that are unique to each organization. The buffer overflow in the Advantech ADAM OPC Server ActiveX control could allow remote attackers to execute arbitrary code and gain/elevate privileges to the currently logged in user. ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their environment, architecture, and product implementation.

BACKGROUND

Advantech is a Taiwanese-based company that manufactures and sells industrial personal computers (PCs), embedded computers, automation controllers, and software to customers in the energy, telecommunications, and transportation industries.

According to Advantech, OPC Server is an interface for industrial device servers. The Advantech ADAM OPC server allows Input/Output (I/O) devices to communicate with a wide range of human-machine interface (HMI)/supervisory control and data acquisition (SCADA) software packages. Any software system with OPC client capabilities can access the Advantech OPC server drivers. The Advantech ADAM OPC Server is installed primarily in East Asia with a few installations in North America.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

The buffer overflow in the Advantech ADAM OPC Server ActiveX control might allow remote attackers to execute arbitrary code and gain privileges as the currently logged in user.

CVE-2011-1914[a] has been assigned to this vulnerability.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT

No known exploits specifically target this vulnerability.

DIFFICULTY

An attacker with a low skill level can create a denial of service; however, a more skilled attacker could execute arbitrary code.

MITIGATION

Advantech has created a patch[b] to mitigate this vulnerability. ICST has tested the patch to verify that the vulnerability has been corrected. The patches for the three products can be downloaded at the following location: http://support.advantech.com.tw/support/DownloadSRDetail.aspx?SR_ID=1-2NMHLB

In addition to applying the patch developed by Advantech, ICS-CERT encourages asset owners to take additional defensive measures to reduce the cybersecurity risk introduced by this vulnerability.

- 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, and isolate them from the business network.

[a] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-1914.

[b] http://www.advantechdirect.com/emarketingprograms/OPCServer_Patch/OPCServer_Patch.htm, website last accessed November 02, 2011.

- 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.

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. ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

The Control Systems Security Program (CSSP) also provides a recommended practices section for control systems on the CSSP web page. Several recommended practices are available for reading or downloading, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*[c]

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 provided when prior coordination has occurred with either the vendor, ICS-CERT, or other coordinating entity. 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.

[c] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed November 02, 2011.