ICS-CERT ADVISORY

ICSA-12-137-02—ADVANTECH STUDIO ISSYMBOL ACTIVEX BUFFER OVERFLOWS

May 16, 2012

OVERVIEW

This advisory is a follow-up to the original alert titled ICS-ALERT-11-131-01 - Advantech Studio ISSymbol ActiveX Control Buffer Overflow Vulnerabilities that was published May 11, 2011, on the ICS-CERT web page.

A remote attacker could exploit these vulnerabilities; publicly available exploit code is known to exist that targets these vulnerabilities.

Independent researcher Dmitriy Pletnev of Secunia has identified multiple buffer overflow vulnerabilities in the Advantech Studio product. Advantech has produced a new version that mitigates these vulnerabilities. Mr. Pletnev has tested the new version to validate that it resolves the vulnerabilities.

AFFECTED PRODUCTS

The researcher reported that these vulnerabilities affect the following versions of Advantech Studio:

- Advantech ISSymbol ActiveX Control 61.6.0.0, and
- Advantech Studio 6.1 SP6 Build 61.6.01.05.

IMPACT

Successful exploitation of these vulnerabilities could allow an attacker to arbitrarily execute code.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of these vulnerabilities based on their environment, architecture, and product implementation.

BACKGROUND

Advantech Studio is a collection of automation tools that includes components required to develop human-machine interfaces (HMIs) and supervisory control and data acquisition

(SCADA) system applications that run on various Windows platforms. According to Advantech, Advantech Studio is currently being used at nearly 2,000 installations worldwide. Advantech Studio can be used in a variety of applications including remote utility management, building automation, water and wastewater management, and factory automation.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

BUFFER OVERFLOWS

Boundary errors when processing any of four different properties can be exploited to cause buffer overflows, which in turn can allow execution of arbitrary code.

CVE-2011-0340[a] has been assigned to these vulnerabilities.

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities are remotely exploitable.

EXISTENCE OF EXPLOIT

Public exploits are known to target these vulnerabilities.

DIFFICULTY

An attacker with a low skill level can create the denial of service whereas it would require a more skilled attacker to execute arbitrary code.

MITIGATION

Advantech recommends that users of Advantech Studio Version 6.1 and earlier versions upgrade to the new version, Advantech Studio 7.0. Customers should contact their authorized Advantech distributor or their Advantech account manager to discuss the transition plan to Advantech Studio 7.0. Advantech further recommends that users affected by this announcement read the customer notice found at the following link:

http://www.advantechdirect.com/eMarketingPrograms/AStudio_Patch/AStudio7.0_Patch_Final.htm

a. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0340, website last accessed May 16, 2012.

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, 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.

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 section for control system 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.[b]

ICS-CERT CONTACT

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

b. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed May 16, 2012.