ICS-CERT ADVISORY

ICSA-10-337-01—ADVANTECH STUDIO TEST WEB SERVER BUFFER OVERFLOW

January 03, 2011

OVERVIEW

The ICS-CERT has received a report from independent security researcher Jeremy Brown that reveals a stack-based buffer overflow vulnerability in the test web server bundled with Advantech Studio Version 6.1. This web server is intended to be used for testing purposes and should not be used in a production environment. Advantech has verified the problem and has developed a patch to mitigate the vulnerability.

AFFECTED PRODUCTS

This vulnerability affects the test web server bundled with Advantech Studio Version 6.1 and all previous versions. This does not apply to Windows CE versions.

IMPACT

Advantech recommends using the bundled test web server only for testing purposes. If the bundled test web server is not used in production, the impact of this vulnerability should be minimal.

While a successful exploit of the buffer overflow could allow arbitrary code execution, the specific impact to an individual organization depends on many factors that are unique to the organization. ICS-CERT recommends that organizations evaluate the impact of this vulnerability 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 System (SCADA) applications that run on various Windows platforms. According to Advantech, Advantech Studio is currently being used in 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

The Advantech Studio bundled test web server is vulnerable to a stack-based buffer overflow when more than 2048 bytes are written to the fixed-size stack buffer. When sending a request greater than 2048 bytes, the test web server writes past the bounds of the buffer and corrupts memory, allowing the execution of arbitrary code.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT

There are currently no publicly known exploits specifically targeting this vulnerability.

DIFFICULTY

An attacker would require an intermediate skill level to exploit this vulnerability.

MITIGATION

If the bundled test web server is being used in a production environment, Advantech recommends migrating to Microsoft Internet Information Services (IIS).

Advantech further recommends that users of Advantech Studio take the following mitigation steps:

- Upgrade to the latest version and install the patch. The patch can be applied to Advantech Studio Version 6.1 and any earlier version. Users can get more information and download the patch at:

  http://www.advantechdirect.com/emarketingprograms/AStudio_Patch/AStudio_Patch.htm

- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet. [1]
- Control system networks and devices should be located behind firewalls, and be isolated from the business network. If remote access is required, secure methods such as Virtual Private Networks (VPNs) should be utilized.

1. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, website last visited December 3, 2010.

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 System Security Program also provides a recommended practices section for control systems on the United States Computer Emergency Readiness Team (US-CERT) web site. Several recommended practices are available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*[2]

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

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.

2. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html.