ICS-CERT ADVISORY

ICSA-12-081-01—INVENSYS WONDERWARE SYSTEM PLATFORM BUFFER OVERFLOWS

March 30, 2012

OVERVIEW

ICS-CERT originally released Advisory ICSA-12-081-01P on the US-CERT secure portal on March 21, 2012. This web page release was delayed to allow users time to download and install the update.

Independent researcher Celil Unuver from SignalSec Corporation[a] has identified two buffer overflow vulnerabilities in the WWCabFile component of the Wonderware System Platform, which is used by multiple applications that run on the platform. Invensys has produced a patch that resolves these vulnerabilities. Mr. Unuver has tested the patch and verified that it resolves the vulnerabilities.

AFFECTED PRODUCTS

- The following Invensys products and versions are affected:
- Wonderware Application Server 2012 and all prior versions
- Foxboro Control Software Version 3.1 and all prior versions
- InFusion CE/FE/SCADA 2.5 and all prior versions
- Wonderware Information Server 4.5 and all prior versions
- ArchestrA Application Object Toolkit 3.2 and all prior versions
- InTouch 10.0 to 10.5 only (earlier versions of InTouch are not affected).

NOTE: The Wonderware Historian is part of the System Platform but is not affected by this Security Update.

a. SignalSec, http://www.signalsec.com/, website last accessed March 30, 2012.

IMPACT

Successfully exploiting these vulnerabilities will cause a buffer overflow that may allow remote code execution.

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 operational environment, architecture, and product implementation.

BACKGROUND

Wonderware System Platform, along with the Foxboro Control Software, is used for designing, building, deploying, and maintaining standardized applications for manufacturing and infrastructure operations. The Wonderware Information Server is a component of the System Platform and is used for aggregating and presenting plant production and performance data.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

HEAP-BASED BUFFER OVERFLOW[b]

A heap-based overflow can be used to overwrite function pointers that exist in memory with pointers to the attacker's code. Applications that do not explicitly use function pointers are still vulnerable, as unrelated run-time programs can leave operational function pointers in memory.

The heap-based buffer overflow in WWCabFile ActiveX Component can be exploited by sending a long string of data to the "Open" member of the WWCabFile component.

Common Vulnerabilities and Exposures (CVE) Identifier CVE-2012-0257[c] has been assigned to this vulnerability. According to Invensys, a CVSS V2 base score of 6.0 has also been assigned.

HEAP-BASED BUFFER OVERFLOW

The heap-based buffer overflow can be exploited by sending a long data string to the "AddFile" member of the WWCabFile component.

CVE Identifier CVE-2012-0258[d] has been assigned to this vulnerability. According to Invensys, a CVSS V2 base score of 6.0 has also been assigned.

b. http://cwe.mitre.org/data/definitions/122.html, website last accessed March 30, 2012.
c. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0257, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.
d. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0258, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities require user interaction to exploit, possibly by social engineering.

EXISTENCE OF EXPLOIT

No known public exploits specifically target these vulnerabilities.

DIFFICULTY

Invensys has rated these vulnerabilities as a medium concern based on exploit difficulty and the potential that social engineering may be required.

MITIGATION

Invensys encourages users affected by these vulnerabilities to follow the instructions in their security bulletin, found here:
https://wdnresource.wonderware.com/support/docs/_SecurityBulletins/Security_Bulletin_LFSEC00000071.pdf

Installation of the Security Update does not require a reboot. If multiple products are installed on the same node, the customer need only install the Security Update once.

To install the update, Invensys recommends users to follow the instructions found in the ReadMe file for the product and component being installed. In general, Invensys recommends that users:

Back up the Galaxy Database

Back up the Wonderware Information Server Database

Run the Security Update Utility.

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.

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.*[e] 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*[f] for more information on avoiding e-mail scams
3. Refer to *Avoiding Social Engineering and Phishing Attacks*[g] for more information on social engineering attacks.

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.

e. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed March 30, 2012.
f. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed March 30, 2012.
g. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed March 30, 2012.