# ICS-CERT ADVISORY

## ICSA-12-171-01—WONDERWARE SUITELINK UNALLOCATED UNICODE STRING VULNERABILITY

June 19, 2012

## OVERVIEW

This Advisory is a follow-up to the original ICS-CERT Alert titled ICS-ALERT-12-136-01 - Wonderware SuiteLink Unallocated Unicode String that was published May 15, 2012 on the ICS-CERT web page.

Independent researcher Luigi Auriemma identified a maliciously crafted Unicode string vulnerability causing a stack-based buffer overflow with proof-of-concept (PoC) exploit code that affects the Invensys Wonderware SuiteLink service (slssvc.exe). This vulnerability was released without coordinating with ICS-CERT or the vendor. This vulnerability can be exploited remotely, and public exploits are known to target this vulnerability. Wonderware SuiteLink is part of the System Platform software suite.

ICS-CERT has coordinated this vulnerability with Invensys. Invensys has confirmed the vulnerability exists for Wonderware products built prior to 2011. Invensys has produced a patch that resolves this vulnerability. This patch validation was confirmed by Luigi Auriemma.

## AFFECTED PRODUCTS

All Wonderware products built prior to 2011 are affected:

- slssvc service less than or equal to Version 54.x.x.x is vulnerable, and
- slssvc service equal to or greater than Version 58.x.x.x is not vulnerable.

Slssvc service Versions 55–57 were never publicly released. InTouch 2012 and Wonderware Application Server 2012 are not vulnerable to crash but will show excessive resource consumption if exploited.

## IMPACT

The vulnerability allows an attacker to cause a buffer overflow that can ultimately lead to a denial-of-service (DoS) and crash of the system in some versions.

The vulnerability allows an attacker to remotely stall or crash the slssvc service by sending a long and unallocated Unicode string to the buffer. This exploit could affect critical infrastructure and key resources where Wonderware SuiteLink is deployed.

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 operational environment, architecture, and product implementation.

## BACKGROUND

SuiteLink is a common component used for communication between Wonderware products. It is also used for communication between Wonderware products and some third-party products developed with Wonderware's Extensibility Tool Kits. The Invensys Wonderware SuiteLink Service connects Wonderware software with third-party products and OPC-compliant devices and applications. Generally, when a Wonderware product is installed, SuiteLink is likely also installed as a common component. The SuiteLink service is a common component of the System Platform used to transport value, time, and quality of digital I/O information and extensive diagnostics with high throughput between industrial devices, third party, and Wonderware products.

The Invensys[a] Wonderware SuiteLink component is deployed in many industries worldwide, including manufacturing, energy, food and beverage, chemical, and water and wastewater.

# VULNERABILITY CHARACTERIZATION

## VULNERABILITY OVERVIEW

### STACK-BASED BUFFER OVERFLOW[b]

Attackers can send an oversized unallocated string into the SuiteLink buffer that causes the allocated stack buffer to be overwritten. This attack causes a crash of slssvc.exe and a DoS.

CVE-2012-3007[c] has been assigned to this vulnerability. A CVSS V2 base score of 7.1 has also been assigned (AV:N/AC:M/Au:N/C:N/I:N/A:C).[d]

a. Invensys, http://www.invensys.com/, Web site last accessed June 19, 2012.

b. CWE-121: Stack Based Buffer Overflow, http://cwe.mitre.org/data/definitions/121.html, Web site last accessed June 19, 2012.

c. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3007 , NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

## VULNERABILITY DETAILS

### EXPLOITABILITY

This vulnerability is remotely exploitable.

### EXISTENCE OF EXPLOIT

Public exploits are known to target this vulnerability.

### DIFFICULTY

An attacker with a low skill level would be able to exploit this vulnerability.

## MITIGATION

Invensys recommends the following mitigations.

- Apply security update patch to affected nodes.
- Upgrade to InTouch/Wonderware Application Server (IT 10.5, WAS 3.5) or later.
- Upgrade to DASABCIP 4.1 SP2 or DASSiDirect 3.0.
- Install DAServer Runtime Components Upgrade 3.0 SP2, 3.0 SP3 or higher for any DAServer, DI Object, or third-party DAServer installation.

The Invensys security update patch can be found at the Wonderware download Web site.[e] Customers can refer to Invensys Security Central for further security information.

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.

d. CVSS Score, http://nvd.nist.gov/cvss.cfm?adv&name=&vector=%28AV:N/AC:M/Au:N/C:N/I:N/A:C%29&version=2, Web site last accessed June 19, 2012.

e. Wonderware SuiteLink security update patch location, https://wdn.wonderware.com/sites/WDN/Pages/Downloads/Software.aspx, Web site last accessed June 19, 2012.

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.[f] 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.

## 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.

f. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed June 19, 2012.