ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
CONTROL SYSTEMS SECURITY PROGRAM

ICS-CERT ALERT

ICS-ALERT-12-136-01—WONDERWARE SUITELINK UNALLOCATED UNICODE STRING

May 15, 2012

ALERT

SUMMARY

ICS-CERT is aware of a public report identifying an unallocated Unicode string vulnerability with proof-of-concept (PoC) exploit code that affects the Invensys Wonderware SuiteLink (SL) service (slssvc), which is part of the System Platform software suite. SuiteLink is a communications protocol used by Invensys Wonderware supervisory control and data acquisition/human-machine interface (SCADA/HMI) products. According to this report, the vulnerability allows an attacker to remotely crash older versions of the slssvc service by sending a long and unallocated Unicode string. This report was released by Luigi Auriemma without coordination with either the vendor or ICS-CERT.

Invensys has confirmed that the vulnerability exists for certain versions of Wonderware InTouch and Wonderware Application Server (WAS) prior to the latest 2012 release. Invensys has identified mitigations for other products and prior versions.

The report included vulnerability details and PoC exploit code for the following vulnerability:

Vulnerability Type	Exploitable	Impact
Unallocated Unicode string	Can be remotely exploited	Denial of Service

This ICS-CERT alert provides early notice of the report and identifies baseline mitigations for reducing risks to these and other cybersecurity risks. ICS-CERT is currently working with the security researcher and Invensys regarding mitigations to resolve this issue.

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

MITIGATION

Invensys is working to release a standalone update tool that will provide an upgrade path for all products using the SuiteLink component. Customers that require an immediate mediation can upgrade to the following product versions or install the following products to update SuiteLink and resolve this vulnerability on any affected node:

- InTouch/Wonderware Application Server (IT 10.5, WAS 3.5) or later,
- DASABCIP 4.1SP2 (the first product to ship secured version of SuiteLink),
- DASSiDirect 3.0, and
- DASRTC 3.0SP2 or DASRTC 3.0SP3 upgrade for any DAServer or DIObject or third-party toolkit server.

Customers can access these updates at the following Web site:

https://wdn.wonderware.com/sites/WDN/Pages/Downloads/Software.aspx

Customers should follow the recommendations detailed in the Securing Industrial Control Systems guide available to all customers from the Wonderware Security Central Web site.

ICS-CERT recommends that users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should:

- Follow the Wonderware guidelines for Securing Industrial Control Systems.
- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.[b]
- Locate control system networks and devices behind firewalls, and isolate them from the business network.
- If remote access is required, employ secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

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

[a] http://www.invensys.com/, Web site last accessed May 11, 2012.

[b] ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, Web site last accessed May 14, 2012.

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

Organizations that observe 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

ICS-CERT Operations Center
1-877-776-7585
Email: ics-cert@dhs.gov

For CSSP Information and Incident Reporting: www.ics-cert.org

DOCUMENT FAQ

What is an ICS-CERT Alert? An ICS-CERT Alert is intended to provide timely notification to critical infrastructure owners and operators concerning threats 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.

[c] Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed May 14, 2012.