Invensys Operations Management Security Alert

Title

SuiteLink Service (SLSSVC) Vulnerability (LFSEC 00000038 - UPDATED)

Rating

Medium

Published By

Invensys Operations Management Security Response Center

Overview

Invensys is aware that a denial of service type vulnerability, including exploit code, has been posted on the web against the Wonderware SuiteLink service (slssvc.exe), which 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, 3rd party, and Wonderware products.

Invensys has confirmed the vulnerability exists for Wonderware products built prior to 2011. Slssvc.exe can be crashed when a very long and unallocatable unicode string is sent to the service remotely. Mitigations for Wonderware and other products that carry SuiteLink have been identified for all supported versions.

To determine if a system is vulnerable, inspect the file version of the SuiteLink service located at "\Program Files\Common Files\Archestra\slssvc.exe" on 32-bit OS and "\Program Files (x86)\Common Files\Archestra\slssvc.exe" on 64-bit OS. If the file version is:

- Equal to or Less than 54.x.x.x, then the system **is** vulnerable.
- Greater than or equal to 58.x.x.x then the system is **not** vulnerable.
- Versions 55-57 have not been released to market so you will not encounter those.

The SuiteLink version shipped with InTouch 2012 and WAS 2012 is not vulnerable to a crash but will show excessive resource consumption if exploited.

Invensys is preparing a Security Update that mitigates the identified denial of service vulnerability and can be installed on all supported versions of Wonderware products that use the SuiteLink service. Since this is a common component, Wonderware recommends the installation of this security update on all Wonderware product nodes that use SuiteLink communication.

Mitigation Recommendations

Customers that require an immediate mitigation may upgrade to the following product versions or install the following products on any affected node to update SuiteLink and fix this vulnerability:

• InTouch/Wonderware Application Server (IT 10.5, WAS 3.5) or later

• DASABCIP 4.1 SP2 or DASSiDirect 3.0

• DAServer Runtime Components Upgrade 3.0 SP2, 3.0 SP3 or higher for any DAServer, DI Object or third-party DAServer installation.

As always, customers should follow the recommendations detailed in the "Securing Industrial Control Systems" guide available to all customers via the Wonderware Security Central/Cyber Security Updates website.

Good common practice 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.

• 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.

The Security Update that can be used to patch all affected nodes is available for download at the following website: https://wdn.wonderware.com/sites/WDN/Pages/Downloads/Software.aspx. Expand the **General** item, then click **SuiteLink 2.0 SP2**.

NVD Common Vulnerability Scoring System

The U.S. Department of Homeland Security has adopted the common Vulnerability Scoring System (CVSS) that provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. The system is comprised of components: impact, exploitability and complexity as well as added determinants such as authentication and impact type. In summary, the components such as impact are given an individual score between 0.0 and 10.0. The average of all components is the overall score where the maximum is 10.0. Details about this scoring system can be found here: http://nvd.nist.gov/cvss.cfm

Our assessment of the vulnerability using the CVSS Version 2.0 calculator rates an Overall CVSS Score of 5.6. To review the assessment, use this link: **National Vulnerability Database Calculator for LFSEC00000038** . Customers have the option in the Environmental Score Metrics section of the calculator to further refine the assessment based on the organizational environment of the installed product. Adding the Environmental Score Metrics will assist the customer in determining the operational consequences of this vulnerability on their installation.[1]

Affected Products and Components[2]

All Wonderware products released **prior to June 2011** are affected on all operating systems except those noted below.

Non-Affected Products

- InTouch/Wonderware Application Server (IT 10.5, WAS 3.5) or later
- DASABCIP 4.1SP2

[1] CVSS Guide

[2] Registered trademarks and trademarks must be noted such as "Windows Vista and Windows XP are trademarks of the Microsoft group of companies."

- DASSiDirect 3.0
- DAServer Runtime Components Upgrade 3.0SP2 or DAServer Runtime Components Upgrade 3.0SP3 upgrade

Vulnerability Characterization

A buffer overflow is a programming error where data larger than the allocated memory space overwrites adjacent memory. There are two types, stack based and heap based, the latter of which is much more difficult to exploit.

Any machine where the SLSSVC service is installed is affected and must be patched or updated to the newer version. No other components of the System Platform are affected.

Update Information

An updated Security Bulletin will be released on Security Central with details on installing the Security Update.

Other Information

Acknowledgments

The vulnerability report and associated proof of concept exploit code was released by Luigi Auriemma without coordination with either ICS-CERT or Invensys. However, Invensys appreciates anyone that calls attention to vulnerabilities in our products that in turn affect the safety and wellbeing of our customers and their systems. Invensys would like to acknowledge the continued collaboration with ICS-CERT for their expert help in the coordination of this Security Update.

Support

For information on how to reach Invensys Operations Management support for your product, refer to this link: Invensys Customer First Support. If you discover errors or omissions in this bulletin, please report the finding to support.

Invensys Operations Management Cyber Security Updates

For information and useful links related to security updates, please visit the Cyber Security Updates site.

Cyber Security Standards and Best Practices

For information regarding how to secure Industrial Control Systems operating in a Microsoft Windows environment, please reference the Invensys Securing Industrial Control Systems Guide.

Invensys Operations Management Security Central

For the latest security information and events, visit Security Central.

Disclaimer

THE INFORMATION PROVIDED HEREIN IS PROVIDED “AS-IS” AND WITHOUT WARRANTY OF ANY KIND. INVENSYS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY INVENSYS, ITS DEALERS, DISTRIBUTORS, AGENTS OR EMPLOYEES WILL CREATE A WARRANTY AND CUSTOMER MAY NOT RELY ON ANY SUCH INFORMATION OR ADVICE.

INVENSYS DOES NOT WARRANT THAT THE SOFTWARE WILL MEET CUSTOMER’S REQUIREMENTS, THAT THE SOFTWARE WILL OPERATE IN COMBINATIONS OTHER THAN AS SPECIFIED IN INVENSYS’ DOCUMENTATION OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE.

IN NO EVENT WILL INVENSYS OR ITS SUPPLIERS, DEALERS, DISTRIBUTORS, AGENTS OR EMPLOYEES BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY CUSTOMER OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF INVENSYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. INVENSYS’ LIABILITY FOR DAMAGES AND EXPENSES HEREUNDER OR RELATING HERETO (WHETHER IN AN ACTION IN CONTRACT, TORT OR OTHERWISE) WILL IN NO EVENT EXCEED THE AMOUNT OF FIVE HUNDRED DOLLARS ($500 USD).

.