Invensys Operations Management Security Bulletin

Title

WIN-XML Exporter Improper Input Validation Vulnerability (LFSEC00000086)

Rating

High

Published By

Invensys Operations Management Security Response Center

Overview

A *vulnerability* has been discovered in the WIN-XML Exporter component of Wonderware Information Server. This vulnerability, if exploited, could allow attackers to access local resources (files and internal resources) or enable denial of service attacks. The rating is High and may require social engineering to exploit. Social engineering is when people are unknowingly manipulated to perform certain actions that may be detrimental to the system. For example, asking an end-user to click on an email link or download a file.

This security bulletin announces the software updates available to customers that have been tested on:

Wonderware Information Server 4.0 with SP1, Wonderware Information Server 4.5 and Wonderware Information Server 5.0.

Recommendations

Customers using versions of Win-XML Exporter shipped with Wonderware Information Server WIS 4.0 with SP1, WIS 4.5 and WIS 5.0 SHOULD apply the security update to all nodes where the WIN-XML Exporter component is installed. Customers using Win-XML version shipped with WIS 4.0 and earlier must first upgrade to one of the above versions before applying the fix. Installation does not require a reboot.*

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 6.6. To review the assessment, use this link**.**

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]

The following table identifies the currently supported products affected[3]. Software updates can be downloaded from the Wonderware Development Network ("Software Download" area) and the Infusion Technical Support websites using the links embedded in the table below.

Product and Component	Supported Operating System	Security Impact	Severity Rating	Software Update
Wonderware Information Server – WIN XML exporter	Windows2008StdSP2 x32bit	Access to internal network resources, access to the file system, denial of service, path disclosure	6.6	WIS WIN-XML Exporter (LFSEC00000086)
Wonderware Information Server – WIN XML exporter	Windows2008StdSP2 x64bit	Access to internal network resources, access to the file system, denial of service, path disclosure	6.6	WIS WIN-XML Exporter (LFSEC00000086)

Non-Affected Products

- Only nodes where the Win XML exporter component is installed are affected by this vulnerability.

[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."

[3] Customers running earlier versions may contact their support provider for guidance.

Background

Wonderware Information Server provides the full spectrum of industrial information content including process graphics, trends and reports on a single web page.

Wonderware Information Server Web Clients are designed for the more casual user who relies on a Web browser to access real-time dashboards, pre-designed reports of industrial activities as well as the occasional requirement for ad-hoc analysis or write back capabilities to the process.

The Win-XML exporter component of Wonderware Information Server allows the conversion of InTouch windows into XML format so that they can be published to the portal to enable runtime monitoring of the plant floor execution through web clients. This component is usually installed on the machines running the Wonderware InTouch WindowMaker component.

Vulnerability Characterization

The Win-XML exporter component of Wonderware Information Server contains a vulnerability that may allow access to local files and other internal resources by exploiting improper parsing of XML external entities in an unsecure deployment[4]. If an attacker manages to make a victim open a project that contains specially crafted XML, Wonderware Win-XML Exporter will automatically send the contents of local or remote resource to the attacker's server. It also makes possible to conduct denial of service attacks.

Any machine that the Win-XML Exporter component of Wonderware Information Server is installed on is affected and must be patched by first patching the Server and downloading the updated version from the Server as described in the ReadMe. No other components of Wonderware Information Server are affected.

Update Information

Install the Security Update using instructions provided in the ReadMe for the product and component being installed. In general, the user SHOULD follow the ReadMe instructions delivered with the Security Update..

Other Information

Acknowledgments

Invensys thanks the following for the discovery and collaboration with us on this vulnerability:

- Gleb Gritsai, Nikita Mikhalevsky, Timur Yunusov, Denis Baranov, Ilya Karpov, Vyacheslav Egoshin, Dmitry Serebryannikov, Alexey Osipov, Ivan Poliyanchuk, and Evgeny Ermakovof the Positive Technologies team for reporting the Win-XML Exporter XML External Entity Parsing (LFSec00000086)

[4] Any control system installation which does not follow the practices described in the Invensys Securing Industrial Control Systems Guide

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).

.