Invensys Operations Management Security Bulletin

Title

Multiple Vulnerabilities in Wonderware Information Server LFSEC00000091

Rating

Critical

Published By

Invensys Operations Management Security Response Center

Overview

In coordination with Independent researchers Gleb Gritsai, Nikita Mikhalevsky, Timur Yunusov, Denis Baranov, Ilya Karpov, Vyacheslav Egoshin, Dmitry Serebryannikov, Alexey Osipov, Ivan Poliyanchuk, and Evgeny Ermakov of the Positive Technologies Research Team, Invensys has performed a security update of the Wonderware Information Server (WIS) web pages and components to address multiple vulnerabilities including cross-site scripting, file system access, XML Entity Injection, and blind SQL-injection. These vulnerabilities, if exploited, could allow remote code execution, information disclosure or session credential high jacking and are given a rating of “Critical”. There are no known exploits in the wild at this time. These vulnerabilities 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. Impact to individual organizations depends on many factors that are unique to each organization. Invensys recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation.

This security bulletin announces the software updates available to customers that have been tested on Wonderware Information Server as described below:

Security Update for Wonderware Information Server 4.0 SP1 and 4.5
Security Update for Wonderware Information Server 5.0 Server

Recommendations

Customers using versions prior to and including WIS 5.0 are affected. A security update has been released for the versions below. End users SHOULD apply the security update to all nodes where the Information Server Portal is installed. Browser clients of the portal are automatically updated after applying the fix and then visiting the portal.

If Wonderware Information Server 4.0 and earlier versions are used, then those nodes must first be upgraded to one of the above versions before applying the fix.

Customers using the affected versions of Wonderware Information Server SHOULD set the Security level settings in the Internet browser to “Medium – High” to minimize the risks presented by these vulnerabilities.

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 compound vulnerabilities, averaging the CVSS scores from the version 2.0 calculator, rates this security update as critical. See below for specific scoring vectors.

Affected Products and Components[1]

The following table identifies the currently supported products affected[2]. 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 4.0 SP1 and 4.5– Portal	Windows Server 2003 and R2,SPs Windows Server 2008, R2 and SPs Windows 7 SQL 2008 SP1	Remote code execution, information disclosure, session credential high jacking	Critical	WIS 4.0 SP1 and 4.5 (LFSEC00000091)
Wonderware Information Server 5.0 – Portal	Windows XP Professional SP3 Windows Server 2003 and R2, SPs Windows Server 2008 and SPs windows Vista Windows 7	Remote code execution, information disclosure, session credential high jacking	Critical	WIS 5.0 (LFSEC00000091) WIS 5.0 Remote Server (LFSEC00000091a)

Non-Affected Products

- Wonderware Historian Clients
- Wonderware Information Server Clients

[1] Registered trademarks and trademarks must be noted such as "Windows Vista and Windows XP are trademarks of the Microsoft group of companies."
[2] 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. This software is used in many industries worldwide, including critical manufacturing, energy, food and beverage, chemical, and water and wastewater.

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.

Vulnerability Characterization

A cross-site scripting vulnerability can enable an attacker to inject client side script into web pages viewed by other users or bypass client side security mechanisms imposed by modern web browsers.

National Vulnerability Database Calculator for the XXS vulnerability is 9.3: and the CVSS vector string is (AV:N/AC:M/Au:N/C:C/I:C/A:C).

A SQL injection vulnerability can be used by an attacker to perform database operations that were unintended by the web application designer and in some instances can lead to total compromise of the database server or lead to remote code execution.

National Vulnerability Database Calculator for the XXS vulnerability is 9.3: and the CVSS vector string is (AV:N/AC:M/Au:N/C:C/I:C/A:C).

Improper Input Validation

Wonderware Information Server may allow access to local resources (files and internal resources) via unsafe parsing of XML external entities. By using specially crafted XML files, an attacker can cause these products to send the contents of local or remote resources to the attacker's server or cause a denial of service of the system. This vulnerability is not exploitable remotely and cannot be exploited without user interaction. The exploit is only triggered when a local user runs the vulnerable application and loads the malformed XML files.

National Vulnerability Database Calculator for the XXS vulnerability is 6.3: and the CVSS vector string is (AV:L/AC:M/Au:N/C:C/I:N/A:C).

Resource Exhaustion

Wonderware Information Server does not properly restrict the size or amount of resources that are requested, allowing the attacker to consume more resources than intended. This vulnerability, if exploited, could allow remote code execution and DoS

National Vulnerability Database Calculator for the XXS vulnerability is 9.3: and the CVSS vector string is (AV:N/AC:M/Au:N/C:C/I:C/A:C).

Update Information

Any machine that the Wonderware Information Server Portal is installed is affected and must be patched. Install the Security Update using instructions provided in the ReadMe for the product and component

being installed. Refer to the "Affected Products and Components" section to access the correct link for your product version.

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 Ermakov of the Positive Technologies Research Team for reporting "Multiple Vulnerabilities in WIS Web Pages. LFSEC00000091".

Invensys would also like to acknowledge the continued collaboration with ICS-CERT for their expert help in the coordination of this Security Bulletin.

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/Alerts

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 Wonderware Development Network/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).