Invensys Operations Management Security Bulletin

Title

Cross-Site Scripting and SQL Injection in Wonderware Information Server pages and Memory Management issues in Historian Client controls. LFSEC00000069

Rating

Critical

Published By

Invensys Operations Management Security Response Center

Overview

In coordination with cyber researchers Terry McCorkle and Billy Rios, Invensys has performed a security update of the Wonderware Information Server web pages to address multiple vulnerabilities including cross-site scripting and SQL-injection. In addition, memory management issues for the downloaded Historian Client controls were also addressed. 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.

This security bulletin announces the software updates available to customers that have been tested on Wonderware Information Server 4.0 with SP1 and 4.5.

Recommendations

Customers using versions of the products prior to Wonderware Information Server 5.0 and Wonderware Historian Client 10 SP3 SHOULD apply the security update to all nodes where the Information Server Portal and Client components are installed. (All browser clients of the portal are affected and SHOUD be patched).

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 using the CVSS Version 2.0 calculator rates an Overall CVSS Score of 8.1. To review the assessment, use this link: National Vulnerability Database Calculator for LFSEC00000069 . 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 4.0 with 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/ Spoofing	8.1	https://wdn.wonderware.com/sites/WDN/Pages/Downloads/Software.aspx
Wonderware Information Server 4.0 with SP1 and 4.5 – Client	Windows XP Professional SP3 Windows Server 2003 and R2, SPs Windows Server 2008 and SPs windows Vista Windows 7	Remote Code Execution/ Spoofing	8.1	https://wdn.wonderware.com/sites/WDN/Pages/Downloads/Software.aspx
Wonderware Historian Client (*)	Windows XP Professional SP3 Windows Server 2003 and R2, SPs Windows Server 2008 and SPs windows Vista Windows 7	Remote Code Execution/ Spoofing	8.1	https://wdn.wonderware.com/sites/WDN/Pages/Downloads/Software.aspx

Non-Affected Products

- (*) Only Wonderware Historian Client versions installed on the same node as Wonderware Information Server Portal or Client are subject to the vulnerabilities reported in this bulletin

Background

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

[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.

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. 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. Memory management issues with client controls can lead to remote code execution of denial of service.

Any machine that the Wonderware Information Server Portal and client components, in conjunction with Wonderware Historian Client are installed on is affected and must be patched, as described in the following section.

Update Information

Install the Security Update using instructions provided in the ReadMe for the product and component being installed. In general, the user SHOULD proceed as indicated below:

1. Wonderware Information Server – portal component: Run the “Hotfix Install Utility”

2. Wonderware Information Server – Client component: Uninstall the client from Add/Remove Programs (ClientSetup.msi), clear the IE cache (see specific instructions in the Readme file provided with the Security Update) and access the Wonderware Information Server site

3. Wonderware Historian Client Desktop only: No action required

4. If #2 and #3 are on the same node, perform the steps in #2 and also Run the “Hotfix Install Utility.”

Other Information

Acknowledgments

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

Billy Rios and Terry McCorkle as independent security researchers for reporting the Wonderware Information Server (LFSEC0000069) Multiple Cross site Scripting, SQL Injection and Memory Management Issues.

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).

.