Invensys Operations Management Security Bulletin

Title

Buffer Overflow in RDBCMI.RuntimeDB.1 and WWView Active X Controls (CR LFSEC00000012)

Rating

Published By

Invensys Operations Management Security Response Center

Overview

Two *vulnerabilities* have been discovered in the Wonderware Information Server client side RDBCMI.RuntimeDB.1 and WWView ActiveX controls. These vulnerabilities, if exploited, could cause a stack based buffer overflow that might allow remote code execution on client machines of Wonderware Information Server versions 3.1, 4.0, 4.0 SP1 and older versions of the product.

The severity rating for these vulnerabilities is “High”, but may require the use of social engineering techniques to effectively exploit them. 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 to a rogue site or to download a malicious file.

This security bulletin announces that software updates are available to customers running Wonderware Information Server 3.1, and Wonderware Information Server 4.0 SP1. Please refer to the “Affected Products and components” section to access the updates.

Recommendations

End users should uninstall the client side components from all client nodes of affected versions of Wonderware Information Server using the Control Panel, Add/Remove Programs applet. Download and install the update to the Portal Server from the specified location for your version of the product. (4.0 users must first install the service pack before installing the update). The updated controls will be reinstalled upon the end user’s next visit to the portal.

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.

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

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

For the ActiveX controls detailed in this bulletin, our assessment of the vulnerabilities using the CVSS Version 2.0 calculator rates an Overall CVSS Score of 6.0. To review the assessment, use this link:

http://nvd.nist.gov/cvss.cfm?name=&vector=(AV:N/AC:H/Au:N/C:C/I:C/A:C/E:P/RL:O/RC:C)&version=2

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 these vulnerabilities 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 using the links embedded in the table below.

Product and Component	Supported Operating System	Maximum Security Impact	Severity Rating	Software Updates
Wonderware Information Server 3.1, 4.0 and 4.0 SP1– Clients (LFSEC00000012)	Windows XP Professional Windows Server 2003 and SPs Windows Server 2003 R2 and SPs Windows Server 2008 and SPs	Remote Code Execution	High	• Wonderware Information Server 3.1 Security Update LFSEC00000012 • Wonderware Information Server 4.0, and 4.0 SP1 Security Update LFSEC00000012

[2] 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.

Not Affected Products and components

Wonderware Information Server versions 4.5 and higher are not affected by this vulnerability.

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

The Wonderware Information Server RDBCMI.RuntimeDB.1 and WWView Client-side ActiveX Controls contain vulnerabilities that may lead to remote Code Execution.

All end users of versions of Wonderware Information Server portal older than 4.5 are affected by this vulnerability as the client side components are downloaded and installed upon the first visit to the portal.

ArchestrA Web Graphics are not affected by the vulnerability reported here.

Other Information

Acknowledgments

Invensys thanks the following for their discovery of, and collaboration with us to resolve, this vulnerability:

- Billy Rios and Terry McCorkle as independent Security Researchers for reporting the Stack Based buffer overflows
- Along with the continual support and collaboration from the ICS-CERT.

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).

.