Date: 8/15/2014

Wonderware Security Bulletin

Title

Multiple Vulnerabilities in Wonderware Information Server LFSEC00000102

Rating

Critical

Published By

Schneider Electric Security Response Center

Overview

In coordination with independent researcher Positive Technologies, Wonderware by Schneider Electric has created a security update for Wonderware Information Server (WIS) web pages and components to address multiple vulnerabilities including cross-site scripting, XML Entity injection, SQL injection, weak encryption and storage of SQL Accounts, and hard-coded credentials.

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 which 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. Schneider Electric recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation.

This security bulletin announces the software security update for Wonderware Information Server 5.5 Server only. If you are on an earlier version of Wonderware Information Server, you must upgrade to Wonderware Information Server 5.5 and apply the Security Update.

Recommendations

Customers using all versions of Wonderware Information Server are affected and should upgrade to Wonderware Information Server 5.5 and then apply the security update.

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. In addition, the Wonderware Information Server Portal can be configured to use HTTPS which will require additional steps as documented in the products user documentation.

Background

Wonderware Information Server provides industrial information content including process graphics, trends and reports on a single web page. This software is used in many industries worldwide, including manufacturing, energy, food and beverage, chemical, and water and wastewater management.

Security Update

August 15, 2014: Wonderware Information Server version 5.5 Security Update addresses the vulnerabilities outlined in this Security Bulletin. You can click here to download the security update for Wonderware Information Server 5.5.

Affected Products and Components[1]

The following table identifies the currently supported products affected. Software updates can be downloaded from the Wonderware Development Network “Software Download” area.

Product and Component	Supported Operating System	Security Impact	Severity Rating	Software Update
Wonderware Information Server 4.0 SP1, 4.5, and 5.0 Portal	Windows Server 2003 and 2012 R2,SPs Windows Server 2008, R2 and SPs Windows 7 SQL 2008 SP1	remote code execution, information disclosure, session credential high jacking	Critical	No Update Available – You must upgrade to Wonderware Information Server v5.5 and apply the Security Update
Wonderware Information Server 5.5 Portal	Windows Server 2003 and 2012 R2, SPs Windows Server 2008 and SPs windows Vista Windows 7	remote code execution, information disclosure, session credential high jacking	Critical	Multiple Vulnerabilities in Wonderware Information Server (LFSEC00000102)

Update Information

All versions of Wonderware Information Server Portal are affected and must be upgraded to Wonderware Information Server 5.5 with the Security Update. Install the Wonderware Information Server 5.5 Security Update using instructions provided in the ReadMe.

Unaffected Products

- **Wonderware Information Server Clients**

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

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 at 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.

Vulnerability Characterization

Cross-Site Scripting

Failure of a site to validate, filter, or encode user input before returning it to a user's web client.

The CVSS for the XXS vulnerability is 7.5 CVSS v2 Vector (AV:N/AC:L/Au:N/C:P/I:P/A:P)

SQL Injection

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 compromise of the database server or lead to remote code execution.

The CVSS for the SQL injection is 7.5 CVSS v2 Vector (AV:N/AC:L/Au:N/C:P/I:P/A:P)

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.

The CVSS for the XML Entity injection is 5.0 CVSS v2 Vector (AV:N/AC:L/Au:N/C:P/I:N/A:N)

Account Encryption and Storage

Weak encryption and storage of accounts may result in an elevation of privilege if an attacker decrypts the credentials. This exploit could occur if the system is compromised by an external attacker.

The CVSS for the Weak Encryption is 2.1 CVSS v2 Vector (AV:L/AC:L/Au:N/C:P/I:N/A:N)

Hard-Coded Credentials

Hard-coded credentials allows an attacker to bypass the authentication that has been configured by the software administrator. This vulnerability might be difficult for the system administrator to detect.

The CVSS for the Hard-Coded credentials is 7.8 CVSS v2 Vector (AV:N/AC:L/Au:N/C:C/I:N/A:N)

Other Information

Acknowledgments

We wish to thank the following researchers for the discovery and collaboration with us on this vulnerability: Timur Yunusov, Ilya Karpov, Sergey Gordeychik, Alexey Osipov, and Dmitry Serebryannikov of the Positive Technologies Research Team for reporting "Multiple Vulnerabilities in Wonderware Information Server LFSEC00000102".

We 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 Customer Support for your product, refer to this link Customer First Support. If you discover errors or omissions in this bulletin, please report the finding to support.

Wonderware 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 Wonderware Securing Industrial Control Systems Guide.

Wonderware Security Central

For the latest security information and events, visit Security Central. (Note that this site requires a login account.).

Disclaimer

THE INFORMATION PROVIDED HEREIN IS PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND. SCHNEIDER ELECTRIC AND ITS AFFILIATES, PARENT AND SUBSIDIARIES (COLLECTIVELY, "SCHNEIDER ELECTRIC") DISCLAIM 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 SCHNEIDER ELECTRIC, ITS DEALERS, DISTRIBUTORS, AGENTS OR EMPLOYEES WILL CREATE A WARRANTY AND CUSTOMER MAY NOT RELY ON ANY SUCH INFORMATION OR ADVICE.

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

IN NO EVENT WILL SCHNEIDER ELECTRIC 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 SCHNEIDER ELECTRIC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SCHNEIDER ELECTRIC'S 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).