Date: 06/23/2015

Wonderware Security Bulletin

Title

InTouch, AppServer, Historian, and SuiteLink Binary Planting Security Vulnerability, LFSEC00000106

Rating

High

Published By

Wonderware|Schneider Electric Security Response Center

Overview

Wonderware by Schneider Electric has created a security update to address Binary Planting vulnerabilities in Wonderware System Platform 2014 R2. The vulnerabilities, if exploited, could allow malicious code execution and are given a rating of “High”. There are no known exploits in the wild at this time. Schneider Electric recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation.

This security bulletin announces the software security update for Wonderware System Platform 2014 R2.

Recommendations

Customers using Wonderware System Platform 2014 R2 and earlier are affected and should apply the Patch 01 update. If you are unable to upgrade to Wonderware System Platform 2014 R2 P01, please follow the recommendations cited in the Wonderware Securing Industrial Control Systems Guide to secure your system.

Background

Wonderware System Platform 2014 R2 acts an “Industrial Operating System” to provide common services such as Configuration, Deployment, Communication, Data Connectivity, Historization, HMI, People Collaboration, and much more. This software is used in many industries worldwide, including manufacturing, energy, food and beverage, chemical, and water and wastewater management.

Security Update

June 16th, 2015: Wonderware System Platform 2014 R2 Patch 01 Update addresses the security vulnerabilities outlined in this Security Bulletin.

Affected Products and Components

The following table identifies the currently supported products affected. Software updates can be downloaded from the Global Customer Support "Software Download" area.

Product and Component	Supported Operating System	Security Impact	Severity Rating	Software Update
Wonderware System Platform 2014 R2	Wonderware System Platform Specifications	Binary Planting, CWE-427	High	WSP2014R2P01
Wonderware System Platform 2014 and earlier	Wonderware System Platform Specifications	Binary Planting, CWE-427	High	Upgrade to WSP2014 R2 and then apply the WSP2014R2P01

Update Information

The Wonderware System Platform 2014 R2 Patch 01 is distributed as an ISO image. The ISO image can be burned to a DVD, mounted as a drive in Virtual Machines, or unpacked to the HDD. To apply the Wonderware System Platform 2014 R2 Patch 01 update to Wonderware System Platform 2014 R2, please follow the installation instructions in the "WSP_Patch_Installation.html" from the ISO image.

Wonderware System Platform 2014 and earlier versions will first need to be upgraded to Wonderware System Platform 2014 R2 and then patched with Wonderware System Platform 2014 R2 Patch 01.

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.

Vulnerability Characterization

- Binary Planting (CWE-427)
  - 7.2 Vector (AV:L/AC:L/Au:N/C:C/I:C/A:C)

Note: Binary Planting is also known as DLL Preloading, DLL Hijacking, and Insecure Library Loading.

Other Information

Acknowledgments

Schneider Electric would like to thank **Ivan Sanchez** and the team from **Wise Security** and **ICS-CERT** for their discovery and cooperation during this vulnerability disclosure process.

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 Security Central

For the latest security information and events, as well as useful links related to security updates, please visit Security Central. *1

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. *1

---

*1 – Site requires a Global Customer Support 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).