Date: 12/19/2014

Wonderware Security Bulletin

Title

InTouch Access Anywhere Server Security Vulnerability, LFSEC00000104

Rating

Critical

Published By

Wonderware|Schneider Electric Security Response Center

Overview

Wonderware by Schneider Electric has created a security update to address a potential vulnerability in the product Wonderware InTouch Access Anywhere Server. This vulnerability, if exploited, could allow remote code execution and is given a rating of “Critical”. There are no known exploits in the wild at this time.

This vulnerability 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 this vulnerability based on their operational environment, architecture, and product implementation.

This security bulletin announces the software security update for Wonderware InTouch Access Anywhere Server version 10.6 and 11.0.

Recommendations

Customers using Wonderware InTouch Access Anywhere Server version 10.6 and 11.0 are affected and should apply the Wonderware InTouch Access Anywhere Server security update.

Background

Wonderware InTouch Access Anywhere Server provides access to InTouch applications through a web browser. This software is used in many industries worldwide, including manufacturing, energy, food and beverage, chemical, and water and wastewater management.

Security Update

December 19, 2014: Wonderware InTouch Access Anywhere Server version 10.6 and 11.0 Security Update addresses the vulnerability outlined in this Security Bulletin. You can click here to download the security update for Wonderware InTouch Access Anywhere Server version 10.6 and 11.0.

Affected Products and Components

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 InTouch Access Anywhere 10.6	Windows Server 2003 and R2, SPs Windows Server 2008 and R2, SPs	Remote Code Execution	Critical	InTouch Access Anywhere Server Security Vulnerability (LFSEC000000104)
Wonderware InTouch Access Anywhere 11.0	Windows Server 2003 and R2, SPs Windows Server 2008 and R2, SPs Windows Server 2012 and SPs	Remote Code Execution	Critical	InTouch Access Anywhere Server Security Vulnerability (LFSEC000000104)

Update Information

Wonderware InTouch Access Anywhere versions 10.6 and11.0 are affected and must be patched with this security update which may be applied to both product versions. Install the Wonderware InTouch Access Anywhere versions 10.6 and 11.0 Security Update using instructions provided in the ReadMe.

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

Remote Code Execution

Stack-based buffer overflow allows remote attackers to execute arbitrary code via a request for a non-existent file.

The CVSS for this vulnerability is 10.0 CVSS v2 Vector (AV:N/AC:L/Au:N/C:P/I:C/A:C)

Other Information

Acknowledgments

We would 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

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).