Date: 03/27/2017

Wonderware Security Bulletin LFSEC00000114

Title

Wonderware InTouch Access Anywhere Multiple Vulnerabilities

Rating

High

Published By

Wonderware|Schneider Electric Security Response Center

Overview

Wonderware by Schneider Electric has created a security update to address vulnerabilities in **Wonderware InTouch Access Anywhere 2014 R2 SP1b (11.5.2) and prior** versions. The vulnerabilities, if exploited, could allow a malicious entity to:

- Perform actions on behalf of a legitimate user
- Perform network reconnaissance
- Gain access to resources beyond those intended with normal operation of the product

Schneider Electric recommends that organizations:

- Evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation
- Apply the provided security patches
- Further secure their systems by applying defense-in-depth techniques

This security bulletin announces the software security update for **Wonderware InTouch Access Anywhere 2014 R2 SP1b (11.5.2) and prior** versions.

Recommendations

Customers using **Wonderware InTouch Access Anywhere 2014 R2 SP1b (11.5.2) and prior** versions of the Server and Gateway components are affected and should upgrade and apply **Wonderware InTouch Access Anywhere 2017 (17.0.0)** as soon as possible.

Background

Wonderware InTouch Access Anywhere enables its users to remotely access a running InTouch application from a desktop computer or a mobile device through an HTML5 enabled browser. This software is used in many industries worldwide, including manufacturing, energy, food and beverage, chemical, and water and wastewater management.

Vulnerability Details

The following four vulnerabilities have been discovered:

1) Cross-Site Request Forgery on the Gateway component of ITAA for multiple state-changing requests. This type of attack requires some level of social engineering in order to get a legitimate user to click on or access a malicious link/site containing the CSRF attack.
2) Ability to specify Arbitrary Server Target Nodes in connection requests to the ITAA Gateway/Access Now Server components.
3) Use of outdated cipher suites and improper verification of peer SSL Certificate
4) Ability to escape out of remote InTouch applications and launch other processes.

Security Update

The following Security Update addresses the vulnerabilities outlined in this Security Bulletin.
03/27/2017: Wonderware InTouch Access Anywhere 2017 (17.0.0)

Affected Products, Components, and corrective Security Patches

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

Product and Component	Supported Operating System	Security Impact	Severity Rating	Software Security Update
Wonderware InTouch Access Anywhere 2014 R2 SP1b (11.5.2) and prior versions	Windows Server 2008, 2008R2, 2012, 2012R2	Confidentiality, Integrity, and some Availability	High	https://gcsresource.invensys.com/tracking/ConfirmDownload.aspx?id=22401

Vulnerability Characterization and CVSSv3 Rating

CWE-352: CSRF, CWE-200: Information Disclosure, CWE-326: Inadequate Encryption Strength

- Cross Site Request Forgery: **8.1 |** CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N
- Arbitrary Server Target Nodes: **6.5 |** CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
- Outdated Cipher Suites/Cert Verification **5.3 |** CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N
- Escaping InTouch Application **5.5 |** CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L

Additional System Hardening

In addition to installing the provided security patch, further steps need to be taken to thoroughly mitigate the vulnerabilities:

- Configure the Wonderware InTouch Access Anywhere Gateway's HTTP Origin Header whitelist to match your environment's URL(s) used for accessing the Gateway. This address may be one or more of the IP, Machine Name, or Fully Qualified Domain Name where the Gateway is hosted. The address may also be that of a Load Balancer or Proxy, if the Gateway is deployed that way.
- Configure the Wonderware InTouch Access Anywhere Gateway's whitelists to restrict access to expected clients IPs, as well as to restrict access from the Gateway to only expected internal server hosts. For an additional defense-in-depth layer, you can further use the Windows OS-level Firewall (or zone firewalls) to restrict communication among only the expected nodes.
- If using self-signed certificates, configure the Wonderware InTouch Access Anywhere Gateway machine to trust the Wonderware InTouch Access Anywhere Server certificate.
- Depending on your organization's requirements, you can further configure the Wonderware InTouch Access Anywhere Gateway to restrict the usable TLS Protocols. For an additional defense-in-depth layer, TLS protocols and cipher suites can also be restricted at the Operating System level through the use of 3rd party tools such as IISCrypto.
- Ensure that you create unique user accounts with minimal privileges dedicated to accessing InTouch applications remotely. OS Group Policy Objects (GPO) can be used to further restrict what those unique user accounts are allowed to do. For an example configuration that disables task manager from being launched in a Remote App connection, follow the steps here.

For detailed instructions on configuring and securing Wonderware InTouch Access Anywhere, please consult with the product's supplied documentation.

Acknowledgements

Schneider Electric would like to thank:

- **Ruslan Habalov** and **Jan Bee** of the **Google ISA Assessments Team** for the discovery and responsible disclosure of these vulnerabilities, the recommendations for fixes, and the verification effort to help ensure the correctness of the patch.
- **ICS-Cert** for coordination of advisories

Support

For information on how to reach Schneider Electric support for your product, please refer to this link: Schneider Electric Software Global Customer Support.

If you discover errors or omissions in this Security Notification, please report the finding to support.

Wonderware Security Central

For the latest security information and security updates, please visit Security Central.

Cyber Security Standards and Best Practices

For information regarding how to secure Industrial Control Systems please reference NIST SP800-82r2.

NVD Common Vulnerability Scoring System (CVSS v3)

The U.S. Department of Homeland Security has adopted the common Vulnerability Scoring System (CVSS v3) that provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. CVSS v3 produces a numerical score as well as a textual representation of that score reflecting the severity of a vulnerability. Scores range from 0.0 (no impact) to a maximum of 10.0 (critical impact with minimal effort to exploit). For additional information please refer to the CVSSv3 specifications.

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 ONE HUNDRED DOLLARS ($100 USD).