Date: 04/28/2017

Wonderware Security Bulletin LFSEC00000120

Title

Wonderware Historian Client XML Injection Vulnerability

Rating

Medium

Published By

Wonderware|Schneider Electric Security Response Center

Overview

Wonderware by Schneider Electric has created a security update to address a vulnerability in **Wonderware Historian Client 2014 R2 SP1 and prior**. The vulnerability, if exploited, could allow a malicious entity to cause denial of service of trend display, or to disclose arbitrary files from the local file system to a malicious web site.

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 Historian Client 2014 R2 SP1.

Recommendations

Customers using Wonderware Historian Client 2014 R2 SP1 are affected and should upgrade and apply HC_SecurityHF_10.6.13100. Customers using older versions of Wonderware Historian Client are also affected and should first upgrade to Wonderware Historian Client 2014 R2 SP1 and then apply HC_SecurityHF_10.6.13100.

Background

Wonderware Historian Client aaTrend provides historized data visualization and trending capabilities. The display configuration settings for aaTrend are stored in XML format. When aaTrend.exe is loading/parsing the configuration settings for a particular display, it is susceptible to XML injection attacks.
Social engineering is required for this attack to be successful. A legitimate user of the system would have to be coerced to select a malicious XML settings file to load.

Security Update

The following Security Updates address the vulnerabilities outlined in this Security Bulletin.
April 28, 2017: HC_SecurityHF_10.6.13100

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 Historian Client 2014 R2 SP1 and prior	Multiple	Confidentiality, Availability	Medium	https://gcsresource.invensys.com/tracking/ConfirmDownload.aspx?id=22409

Vulnerability Characterization and CVSSv3 Rating

CWE-611: Improper Restriction of XML External Entity Reference ('XXE'), CWE-776: Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion'):

- HC 2014 R2 SP1 and prior **6.6 |** CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:H

Acknowledgements

Schneider Electric would like to thank:

- **Andrey Zhukov** from **USSC** for the discovery, responsible disclosure of this vulnerability, and verification of the security 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).