Date: 01/24/2017

Wonderware Security Advisory LFSEC00000115

Title

Historian Default Login Credentials

Rating

High

Published By

Wonderware|Schneider Electric Security Response Center

Overview

Wonderware Historian creates native SQL logins with default passwords, which can allow a malicious entity to compromise Historian databases. In some installation scenarios, SQL resources beyond those created by Wonderware Historian may be compromised as well.

Background

Wonderware Historian creates the following SQL native logins for applications other than Historian to interact with Historian databases and data:

aaUser, wwUser, aaPower, wwPower, aaDbo, wwDbo, aaAdmin, wwAdmin

These logins are created with default credentials within SQL Server. The admin logins (aaAdmin and wwAdmin) further vary in that:

- If Wonderware Historian is installed by itself, the admin logins' privileges are limited to Historian database rights.
- If Wonderware Historian is installed with Wonderware Application Server GR Feature on the same node and Wonderware Application Server is using Legacy Security mode as opposed to Enhanced Security mode, the admin logins' privileges effectively become a sysAdmin.

Affected Products and Components

The following table identifies the currently supported products affected.

Product and Component	Supported Operating System	Security Impact	Severity Rating
Wonderware Historian 2014 R2 SP1 P01 and earlier	Multiple Windows OS	Confidentiality, Integrity, and Availability	High

Vulnerability Characterization and CVSSv3 Rating

CWE-255: Credentials Management.

- Historian only install: **7.3 |** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
- Historian + Application Server install: **9.8 |** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Mitigation

Wonderware Historian software does not make use of any of the created native SQL logins. These logins are only created for software other than Historian to interact with Historian data.

Schneider Electric **strongly recommends** that the following steps be taken to mitigate this vulnerability:

1. Identify where the logins are used. Some likely places for the logins to have been used are:
    a. Wonderware Historian Client
    b. Wonderware InTouch and Application Object scripts
    c. Wonderware Information Server configuration
    d. Custom applications not supplied by Schneider Electric that interact with Historian data
2. Logins that are not used should be disabled from the SQL Server Management Studio
3. For logins that are still in use, the passwords should be changed from the default

For an increased level of security, Schneider Electric and Microsoft further advise that connectivity to SQL Server be accomplished with Windows Integrated Security as opposed to using native SQL logins.

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 this vulnerability
- **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 FIVE HUNDRED DOLLARS ($500 USD).