Date: 02/13/2017

Wonderware Security Bulletin LFSEC00000119

Title

Privilege Escalation in Tableau Server

Rating

Critical

Published By

Wonderware|Schneider Electric Security Response Center

Overview

Wonderware by Schneider Electric has made available a security update to address vulnerabilities in Tableau Server versions 7.0 to 10.1.3, as used by Wonderware Intelligence versions 2014R3 and prior. The vulnerabilities, if exploited, could allow a malicious entity to escalate their privilege to an administrator and take control over the host machine where Tableau Server is installed.

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 Tableau Server version 7.0 to 10.1.3.

Recommendations

Customers using any version of Wonderware Intelligence with Tableau Server 7.0 to 10.1.3 configured for Local Authentication are affected and should apply Tableau Server version 10.1.4 as soon as possible. Analytics Client (Tableau Desktop OEM) should also be upgraded to the same version. Upgrading to Intelligence Server 2014 R3 is recommended but not mandatory as Tableau software works with prior versions of Intelligence data stores.

Even though customers using Wonderware Intelligence Concurrent Licensing for Tableau Server (which requires Active Directory authentication) are not affected by this vulnerability, they may elect to upgrade to the latest releases of Tableau Software using the software update as it is a full installation package.

Background

The Wonderware Intelligence software optionally includes OEM versions of Tableau software, namely Tableau Desktop, branded as the Analytics Client, and Tableau Server branded as the Dashboard Server. The Wonderware Analytics Client enables users to analyze and report on information in the data store created by the Wonderware Intelligence Server, which assembles data from various operational and historical data sources. The Analytics Client publishes dashboards to the Dashboard Server for visualization of various operational metrics and Key Performance Indicators.

When Tableau Server is used with Local Authentication mode, the software is vulnerable due to an administrative account with default credentials that can be used for unauthorized access. If Tableau Server is used with Windows Integrated Security (Active Directory), the software is not vulnerable.

For additional information, please refer to Tableau's security announcement: ADV-2017-001

Security Update

The following Security Update addresses the vulnerabilities outlined in this Security Bulletin:
February 13, 2017: Tableau Server/Desktop 10.1.4

Tableau Server 10.1.4 has been validated with Wonderware Intelligence 2014 R3.

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 Intelligence versions 2014R3 and prior -Tableau Server/Desktop versions 7.0 to 10.1.3	Windows Server 2008, 2008 R2, 2012, 2012R2	Confidentiality, Integrity, and Availability	Critical	Tableau Analytics Dashboard Server v10.1.4 Tableau Analytics Client v10.1.4 Wonderware Intelligence 2014 R3

Vulnerability Characterization and CVSSv3 Rating

CWE-255: Credentials Management.

- Tableau Server with Local Auth — **9.8** | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- Tableau Server with AD Auth — **Not Vulnerable**

Acknowledgements

Schneider Electric would like to thank:
- **Tableau Software** for their timely notification of the security patch availability
- **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).