Wonderware Security Advisory

Title

Tableau OpenSSL Vulnerability (LFSEC00000098)

Rating

High

Published By

Schneider Electric Security Response Center

Overview

A vulnerability has been discovered in the OpenSSL library used by certain versions of Tableau Software Server Components previously posted on WDN. Tableau Software has released security patches for the affected versions.

Tableau Software Server Components that make use of OpenSSL are vulnerable to a buffer error that can result in complete information disclosure of private encryption keys and compromise the security of any of the transmitted data on the Dashboard Server node (Tableau Server).

The rating is High.

This security Advisory announces the Tableau Software updates available to customers that have been tested on Wonderware Intelligence 1.5 SP1.

For detailed information about the HeartBleed vulnerability please refer to the following links:

CVE-2014-0160, http://heartbleed.com/

Recommendations

Customers who have enabled SSL using Tableau Server version 8.0.6 through 8.0.9 or 8.1.0 through 8.1.5 (these would have been installed from WDN as Tableau product updates) should apply the security update to all nodes where the Tableau Dashboard Server is installed. The process consists of un-installing the Dashboard Server and installing the new version. The Server configuration and published dashboards will be preserved during the installation of the new version.

Additionally, it is highly recommended that any certificates used to configure the SSL communication are revoked, new certificates re-acquired, and used after patching the vulnerability. Any passwords used for accessing the server should also be changed after applying the update.

No reboot should be required after these upgrades.

Background

The Tableau analytics software enables users to gather, store, and report on both historical and real-time operational data, using a dashboard to present Key Performance Indicators that are used to visualize, tune and maximize operations.

Security Update

April 2014: Tableau Server **8.1.6** addresses the vulnerabilities outlined in this Security Advisory. You can either:

- Click here to upgrade: Tableau Server 32-bit, or Tableau Server 64-bit.
- Proceed to the Security Updates for version 8.1.6 (following section).

Affected Products and Components[1]

The following table identifies the currently supported products affected[2]. Software updates can be downloaded from the Wonderware Development Network ("Software Download" area) using the links embedded in the table below.

Product and Component	Supported Operating System	Security Impact	Severity Rating	Software Update
Tableau Server component update versions 8.0.6 through 8.0.9 or 8.1.0 through 8.1.5	Windows Server 2003, 2003 R2, 2008, 2008 R2, as well as XP, Vista and Windows 7	Disclosure of information	7.8	Tableau OpenSSL Vulnerability (LFSEC00000098) 32-bit or 64-bit

Non-Affected Products

- Wonderware Intelligence 1.5 and all earlier version as shipped (not updated) are not affected.
- LFSec00000089 and LFSec00000090 security updates to this product are also unaffected.

Update Information

Any machine where the Tableau Server components have been updated to versions 8.0.6 through 8.0.9 or 8.1.0 through 8.1.5 installed from WDN are affected and must be upgraded.

Install the Tableau OpenSSL Vulnerability (LFSEC00000098) using instructions provided in the ReadMe for the product and component being installed. The user must uninstall the older Tableau Server Version and install the newer one.

[1] Registered trademarks and trademarks must be noted such as "Windows Vista and Windows XP are trademarks of the Microsoft group of companies."
[2] Customers running earlier versions may contact their support provider for guidance.

Vulnerability Characterization

The Tableau Server Software components delivered as updates through Wonderware Developers Network (WDN) contain a vulnerability that may allow unauthorized disclosure of information. This vulnerability is characterized as *CWE-119 (Buffer Errors)* that results in disclosure of OpenSSL server memory that could contain encryption keys. This vulnerability, if exploited, allows remote attackers to bypass intended encryption which can result in complete compromise of transmitted data and certificate integrity.

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 here: http://nvd.nist.gov/cvss.cfm

The assessment of the vulnerabilities using the CVSS Version 2.0 calculator based on the deployment environment of Wonderware Intelligence software rates CVSS Scores is as follows:

- The Tableau OpenSSL Vulnerability (LFSEC00000098) has an overall CVSS Score of **7.8**. A detailed CVSS assessment can be found at the following link

Customers have the option in the Environmental Score Metrics section of the calculator to further refine the assessment based on the organizational environment of the installed product. Adding the Environmental Score Metrics will assist the customer in determining the operational consequences of this vulnerability on their installation.[3]

Other Information

Acknowledgments

Schneider Electric thanks the following for the disclosure and collaboration with us on this vulnerability:

- Codenomicon
- Tableau Software
- ICS-Cert

Support

For information on how to reach Schneider Electric support for your product, refer to this link: Customer First Support. If you discover errors or omissions in this Advisory, please report the finding to support.

[3] CVSS Guide

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

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).