



PJM Retiring Use of Weak Encryption

Amanda Egan
Knowledge Management Center
January 13, 2022
Operating Committee

Action Required	Deadline	Who May Be Affected
<p>Update browser settings to TLS 1.2</p> <p>PJM requests that each company update the encryption on the source devices to use an acceptable level of encryption documented in https://www.pjm.com/-/media/etools/security/weak-encryption-remediation-guide.ashx.</p> <p>There is no impact if the company updates the encryption prior to Production deadline.</p>	<p>Production 02/28/2022 6 to 8 pm</p>	<p>Voting Application Users - Voters will not be able to access the voting application (and will not be able to vote) without following the updated procedures provided.</p>



Transport Layer Security (TLS) securely transfers data between clients and servers.
TLS is used to secure data on websites (commonly known as HTTPS).

PJM has determined that using older versions of TLS present a security vulnerability.

TLS 1.0 and TLS 1.1 versions are no longer secure.

- Interception/decryption of secured data is possible when depreciated versions are in use.

PJM will stop supporting TLS 1.0 and TLS 1.1 and will continue supporting only TLS 1.2 in production applications.

- Support for TLS 1.0 and TLS 1.1 will **stop on Feb. 28 for Production Voting Application.**
- **Voting users will not be able to access the application** unless browser settings set to TLS 1.2.
- In the future, PJM will also stop supporting TLS 1.0/1.1 for other PJM Tools, and PJM.com and the browser configuration will globally apply to all applications accessed via the same browser.

Voting users can verify their browser configuration by visiting Voting application (votingtrain.pjm.com) in the Train environment as TLS 1.0 and 1.1 are disabled.

- If a user is prompted with Train SSO login page, their browser is using the correct supported configuration.

If the Voting Application user receives a connection error upon visiting votingtrain.pjm.com, their browser has to be configured.

(<https://help.wheniwork.com/articles/enable-tls-v12-on-your-web-browser/>)

- Personal laptops can be updated by users directly.
- Company help desk engagement might be required for company-issued laptops (due to company restrictions on certain browser settings).

Support for TLS 1.0 and TLS 1.1 will end on Feb. 28 for Production Voting Application.

- A test vote will be issued on March 1 to ensure all Voting application users are able to access the Production Voting Application.

These steps must be taken by Feb. 28, 2022 by all Voting Application users to retain ability to vote

Communication

- Tech Change Forum: December 2021, January, February 2022
- Standing Committees: January, February 2022
- MC Webinar and Forum: January, February 2022

Implementation

- February 28, 2022

Production Testing Period

- March 01, 2022 through March 07, 2022

First Anticipated OC Vote

- March 10, 2022

Presenter:
Amanda Egan,
amanda.egan@pjm.com

SME:
Zeenath Fernandes,
zeenath.Fernandes@pjm.com

Weak Encryption Update



Member Hotline

(610) 666 – 8980

(866) 400 – 8980

custsvc@pjm.com