# Weak Encryption Remediation Update

Zeenath Fernandes
Sr. Lead, Enterprise Information Security

July 13, 2022

PJM © 2022

# Overview

Transport Layer Security (TLS) securely transfers data between clients and servers.

TLS is used to secure data on websites (commonly known as HTTPS).

Older versions of TLS (TLS 1.0 and TLS 1.1) present a security vulnerability.

DHS recommends remediation in an expedited manner.

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

- Interception/decryption of secured data is possible when depreciated TLS 1.0 and TLS 1.1 versions are in use.

PJM has disabled TLS 1.0 and TLS 1.1 in Train Environment since Apr 29 2021 to facilitate stakeholder testing.

PJM has completed disabling TLS 1.0 and TLS 1.1 on several production PJM Tools applications and on PJM.com.

PJM wants to expedite the remediation of remaining PJM Tools applications as per the DHS recommendation.

- **Users will not be able to access the applications** unless browser and browserless API interactions are set to use TLS 1.2.

# Key Dates

| Product | Implementation Date |
|---|---|
| FTR Center | July 19 |
| DR Hub | July 25 |
| Markets Gateway, Capacity Exchange | July 27 |
| Data Viewer, eDART | Aug 01 |
| Power Meter, InSchedule | Aug 10 |
| MSRS, SSO, PJMeSuite | Aug 17 |

# Action Required

## Browser - Action Required

**Latest versions** of web browsers have the TLS 1.2 protocol enabled by default.

To enable TLS 1.2 on web browser versions where TLS 1.2 is not enabled by default, please refer to the respective vendor support documentation.

Browser users can **test** their browser configuration by visiting https://ssotrain.pjm.com/

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

## Browserless/API – Action Required

**Latest versions** of Java and .NET support TLS 1.2 by default.

To enable TLS 1.2 in programming languages where TLS 1.2 is not enabled by default.

- For Java or .NET refer to https://www.pjm.com/-/media/etools/security/weak-encryption-remediation-guide.ashx
- For others, refer to the respective vendor support documentation

Browserless/API users can **test** their configuration by accessing the respective Train Application

# Contact

SME/Presenter:
Zeenath Fernandes,

Zeenath.Fernandes@pjm.com

**Weak Encryption Remediation Update**

Member Hotline

(610) 666 – 8980

(866) 400 – 8980

custsvc@pjm.com

# PROTECT THE POWER GRID

# THINK BEFORE YOU CLICK!

Be alert to malicious phishing emails.

pjm

**Report suspicious email activity to PJM.**

(610) 666-2244 / it_ops_ctr_shift@pjm.com