TCF Special Session on Retiring Weak Encryption

Zeenath Fernandes
Sr. Lead, Enterprise Information Security
March 3, 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).

PJM has determined that use of older versions of TLS presents 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 March 21 for OASIS and ExSchedule Applications.**
- **Users will not be able to access these applications** unless browser and browserless API interactions are set to use TLS 1.2.
- In the future, PJM will also stop supporting TLS 1.0/1.1 for other PJM Tools and PJM.com.

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

Impact Details

Product - Action Required	Deadline	Who May Be Affected
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. **There is no impact if encryption updates are made to the source device prior to the Production deadline.**	**March 21** **5 p.m. to 7 p.m.**	Participants who use PJM's internet facing applications and use weak encryption cipher suites on their source devices. Impacted Tools: Production OASIS and ExSchedule (browser and browserless/API interactions)

Impact Details

Product - Action Required	Deadline	Who May Be Affected
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. **There is no impact if encryption updates are made to the source device prior to the Production deadline.**	**TBD**	Participants who use PJM's internet facing applications and use weak encryption cipher suites on their source devices. Impacted Tools: Account Manager, Billing Line Item Transfer, Bulletin Board, Capacity Exchange, Data Viewer, DER Directory, DR Hub, eCredit, eDART, eGADS, Emergency Procedures, FTR Center, InSchedule, Markets Gateway, MSRS, PJM.com, Planning Center, Power Meter, Resource Tracker, TO Connection, Tools Home

Contact

Facilitator:
Foluso Afelumo, Foluso.Afelumo@pjm.com

Secretary:
Risa Holland, Risa.Holland@pjm.com

SME/Presenter:
Zeenath Fernandes,

Zeenath.Fernandes@pjm.com

Member Hotline

(610) 666 – 8980

(866) 400 – 8980

custsvc@pjm.com

Retiring use of Weak Encryption

PROTECT THE POWER GRID

THINK BEFORE YOU CLICK!

Be alert to malicious phishing emails.

Report suspicious email activity to PJM.

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