

# Retiring use of Weak Encryption

As of March 14, 2022

Zeenath Fernandes

Sr. Lead, Enterprise Information Security

- Production implementation dates for the Account Manager, Tools Home, Bulletin Board, Resource Tracker applications
- Recording of special Tech Change Forum session

Product - Action Required	Deadline	Who May Be Affected
<p>PJM requests that each company update the encryption on the source devices to use an acceptable level of encryption documented in <a href="https://www.pjm.com/-/media/etools/security/weak-encryption-remediation-guide.ashx">https://www.pjm.com/-/media/etools/security/weak-encryption-remediation-guide.ashx</a>.</p> <p><b>There is no impact if encryption updates are made to the source device prior to the Production deadline.</b></p>	<p><b>March 21</b> <b>5 p.m. to 7 p.m.</b></p>	<p>Participants who use PJM’s internet facing applications and use weak encryption cipher suites on their source devices.</p> <p>Impacted Tools: Production OASIS and ExSchedule (browser and browserless/API interactions)</p>



Product - Action Required	Deadline	Who May Be Affected
<p>PJM requests that each company update the encryption on the source devices to use an acceptable level of encryption documented in <a href="https://www.pjm.com/-/media/etools/security/weak-encryption-remediation-guide.ashx">https://www.pjm.com/-/media/etools/security/weak-encryption-remediation-guide.ashx</a>.</p> <p><b>There is no impact if encryption updates are made to the source device prior to the Production deadline.</b></p>	<p><b>April 25</b> <b>6 p.m. to 8 p.m.</b></p>	<p>Participants who use PJM’s internet facing applications and use weak encryption cipher suites on their source devices.</p> <p>Impacted Tools: Account Manager(browser), Tools Home (browser)</p>



Product - Action Required	Deadline	Who May Be Affected
<p>PJM requests that each company update the encryption on the source devices to use an acceptable level of encryption documented in <a href="https://www.pjm.com/-/media/etools/security/weak-encryption-remediation-guide.ashx">https://www.pjm.com/-/media/etools/security/weak-encryption-remediation-guide.ashx</a>.</p> <p><b>There is no impact if encryption updates are made to the source device prior to the Production deadline.</b></p>	<p><b>May 9</b> <b>6 p.m. to 8 p.m.</b></p>	<p>Participants who use PJM’s internet facing applications and use weak encryption cipher suites on their source devices.</p> <p>Impacted Tools: Bulletin Board(browser and browserless/API interactions), Resource Tracker (browser)</p>



Product - Action Required	Deadline	Who May Be Affected
<p>PJM requests that each company update the encryption on the source devices to use an acceptable level of encryption documented in <a href="https://www.pjm.com/-/media/etools/security/weak-encryption-remediation-guide.ashx">https://www.pjm.com/-/media/etools/security/weak-encryption-remediation-guide.ashx</a>.</p> <p><b>There is no impact if encryption updates are made to the source device prior to the Production deadline.</b></p>	<p><b>TBD</b></p>	<p>Participants who use PJM’s internet facing applications and use weak encryption cipher suites on their source devices.</p> <p>Impacted Tools:            Billing Line Item Transfer, 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, TO Connection</p>





# 2022 Roadmap for Retirement of Weak Encryption

2022												
	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Voting		Feb 28										
Account Manager & Tools Home				Apr 25								
OASIS & ExSchedule			Mar 21									
Bulletin Board & Resource Tracker					May 9							

**Legend**

- Start Date
- ◆ End Date

- Recording for March 3<sup>rd</sup> will be made available

## Browser - Action Required

**Latest versions** of web browsers have 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

- National Security Agency (NSA) Recommendation:
  - [Eliminating Obsolete Transport Layer Security \(TLS\)](#)
- 3DES was deprecated by the National Institute of Standards and Technology in 2017. An established reference can be found here:
  - <https://csrc.nist.gov/news/2017/update-to-current-use-and-deprecation-of-tdea>
- TLS 1.0 and TLS 1.1 were released in 1999 and 2006 respectively. Security flaws in design of TLS 1.1 lead to the release of TLS 1.2 in 2008.
  - In October 2018, Apple, Google, Microsoft, and Mozilla jointly announced they would deprecate TLS 1.0 and 1.1 in March 2020.
  - An overview of TLS can be found here:
    - [https://en.wikipedia.org/wiki/Transport\\_Layer\\_Security](https://en.wikipedia.org/wiki/Transport_Layer_Security)
- TLS\_RSA\_\* – Site describing method to attack this cipher suite can be found at <https://robotattack.org/>.

- PJM will no longer support the TLS 1.0 or TLS 1.1 protocols.
- PJM will no longer support the 3DES cipher and the TLS\_RSA\_\* and TLS\_DHE\_RSA\* ciphers in TLS 1.2.
  - Participants need to upgrade the encryption used on systems that connect to PJM externally facing systems.
  - Please see the roadmap slide for details regarding known plans to stop supporting these ciphers on PJM applications
  - Additional details will be provided in the future for the other Tools

- PJM has supplied Weak Encryption Remediation Guide to member companies.
- PJM has shut off weak cipher support in Train (browser and browserless/API) to facilitate member company testing.
- Impacted member company should contact PJM's [member relations](#) to verify list of sources and discuss next steps.
- Questions or feedback can be sent to: [TechChangeForum@pjm.com](mailto:TechChangeForum@pjm.com).

Facilitator:  
Foluso Afelumo, [Foluso.Afelumo@pjm.com](mailto:Foluso.Afelumo@pjm.com)

Secretary:  
Risa Holland, [Risa.Holland@pjm.com](mailto:Risa.Holland@pjm.com)

SME/Presenter:  
Zeenath Fernandes,  
[Zeenath.Fernandes@pjm.com](mailto:Zeenath.Fernandes@pjm.com)

## Retiring use of Weak Encryption



### Member Hotline

(610) 666 – 8980

(866) 400 – 8980

[custsvc@pjm.com](mailto:custsvc@pjm.com)

**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](mailto:it_ops_ctr_shift@pjm.com)

