

Retiring use of Weak Encryption

As of February 14, 2022

Zeenath Fernandes

Sr. Lead, Enterprise Information Security

- Production implementation date for the OASIS and ExSchedule applications
- Additional details on action required
- Information on a 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 https://www.pjm.com/-/media/etools/security/weak-encryption-remediation-guide.ashx.</p> <p>There is no impact if encryption updates are made to the source device prior to the Production deadline.</p>	<p>February 28 5 p.m. to 7 p.m.</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 Voting (browser 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 https://www.pjm.com/-/media/etools/security/weak-encryption-remediation-guide.ashx.</p> <p>There is no impact if encryption updates are made to the source device prior to the Production deadline.</p>	<p>March 21 5 p.m. to 7 p.m.</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 https://www.pjm.com/-/media/etools/security/weak-encryption-remediation-guide.ashx.</p> <p>There is no impact if encryption updates are made to the source device prior to the Production deadline.</p>	<p>TBD</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, 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</p>



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

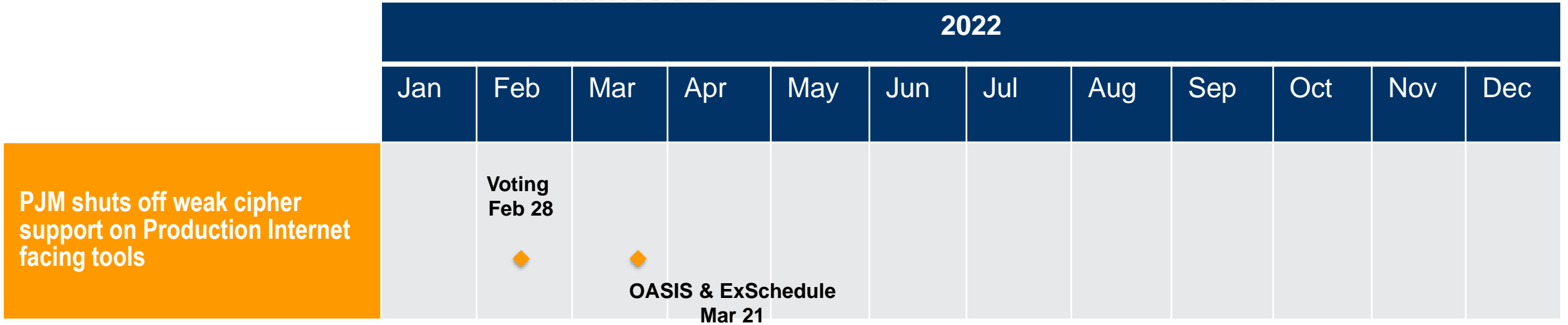
- For Java or .NET refer to <https://www.pjm.com/-/media/etools/security/weak-encryption-remediation-guide.ashx>
- For others, refer to the respective vendor support documentation

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

- Tech Change Forum special session scheduled for March 3
- Focus is on retiring weak encryption
- Register at <https://www.pjm.com/committees-and-groups/forums/tech-change-forum>



2022 Roadmap for Retirement of Weak Encryption



Legend

- Start Date
- ◆ End Date

- 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
- 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.
 - Browser and browserless support for these ciphers will stop for the Voting application on February 28
 - Browser and browserless support for these ciphers will stop for OASIS and ExSchedule on March 21
 - This is necessary due to new NAESEB requirements
 - 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.

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

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

SME/Presenter:
Zeenath Fernandes,
Zeenath.Fernandes@pjm.com

Retiring use of Weak Encryption



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.

Report suspicious email activity to PJM.
(610) 666-2244 / it_ops_ctr_shift@pjm.com

