Retiring use of Weak Encryption

As of November 8, 2021

Zeenath Fernandes

Sr. Lead, Enterprise Information Security

Revisions

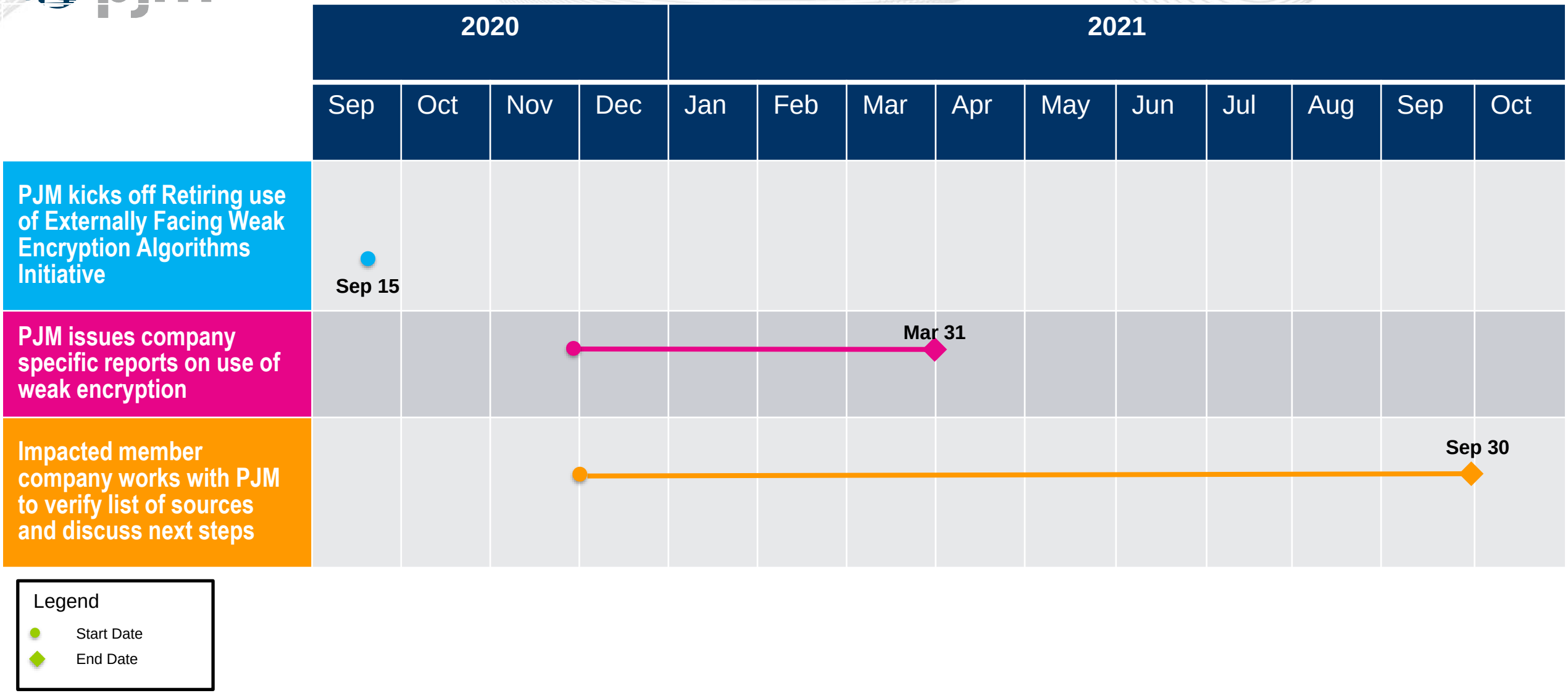
- Production change to disable weak encryption was completed on November 1 for the following products
  - PJM Connect (browser)
  - Gas Pipeline (browser and browserless)

- Production change and list of remaining products in scope for the December 13 change

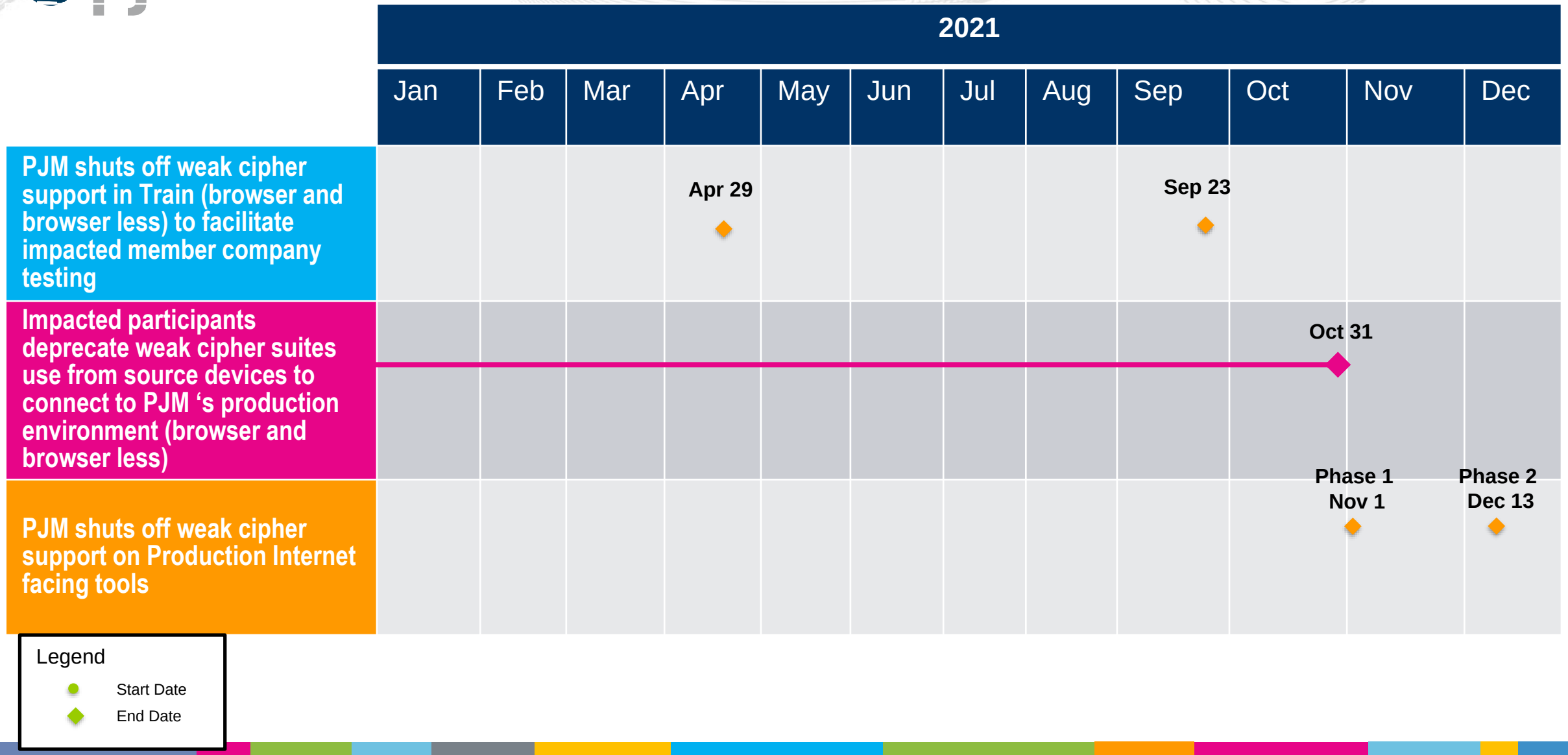
Impact Details

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 the company updates the encryption prior to Production deadline.	**Production (browser and browserless systems)** **December 13** **6 p.m. to 10 p.m.**	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, ExSchedule, FTR Center, InSchedule, Markets Gateway, Messages, MSRS, OASIS, PJM.com, Planning Center, Power Meter, Resource Tracker, TO Connection, Tools Home, Voting

Roadmap for Elimination of Weak Encryption



Roadmap for Elimination of Weak Encryption



Background

- 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/.

Details

- 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.
  - Members need to upgrade the encryption used on systems that connect to PJM externally facing systems.
  - Browser and browser less support will stop on April 29 2021 in Train
  - Browser and browser less support will stop on November 1 2021 in Gas Pipeline and PJM Connect
  - Browser and browser less support will stop on December 13 2021 in other applications

- These encryption mechanisms are no longer secure.

Details

- PJM has supplied Weak Encryption Remediation Guide to member companies.
- PJM has shut off weak cipher support in Train (browser and browser less) 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.

December 13 Impacted Tools

- Account Manager
- Billing Line Item Transfer
- Bulletin Board
- Capacity Exchange
- Data Viewer
- DER Directory
- DR Hub
- eCredit
- eDART
- eGADS
- Emergency Procedures
- ExSchedule
- FTR Center
- InSchedule
- Markets Gateway
- Messages
- MSRS
- OASIS
- PJM.com
- Planning Center
- Power Meter
- Resource Tracker
- TO Connection
- Tools Home
- Voting

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