Retiring use of Weak Encryption

As of October 13, 2021
Zeenath Fernandes
Sr. Lead, Enterprise Information Security

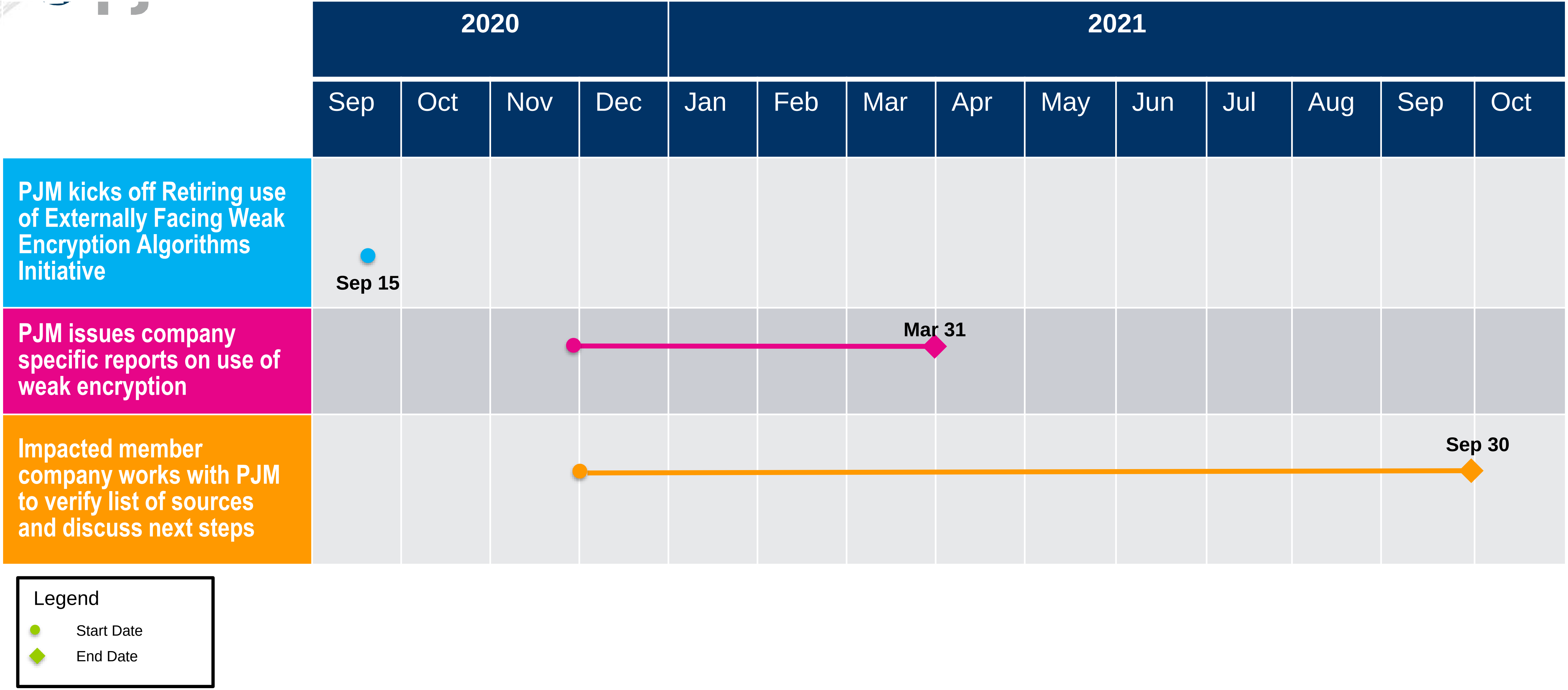
Revisions

- Production change to disable weak encryption for browser and browserless systems will be on November 1

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.	**Production** **(browser and browserless systems)** **November 1** **6 p.m. to 10 p.m.**	• Participants who use PJM's internet facing tools and use weak encryption cipher suites on their source devices. • 94% of encrypted sessions are already strong and are not affected.

Roadmap for Elimination of Weak Encryption



PJM kicks off Retiring use of Externally Facing Weak Encryption Algorithms Initiative

Sep 15

PJM issues company specific reports on use of weak encryption

Mar 31

Impacted member company works with PJM to verify list of sources and discuss next steps

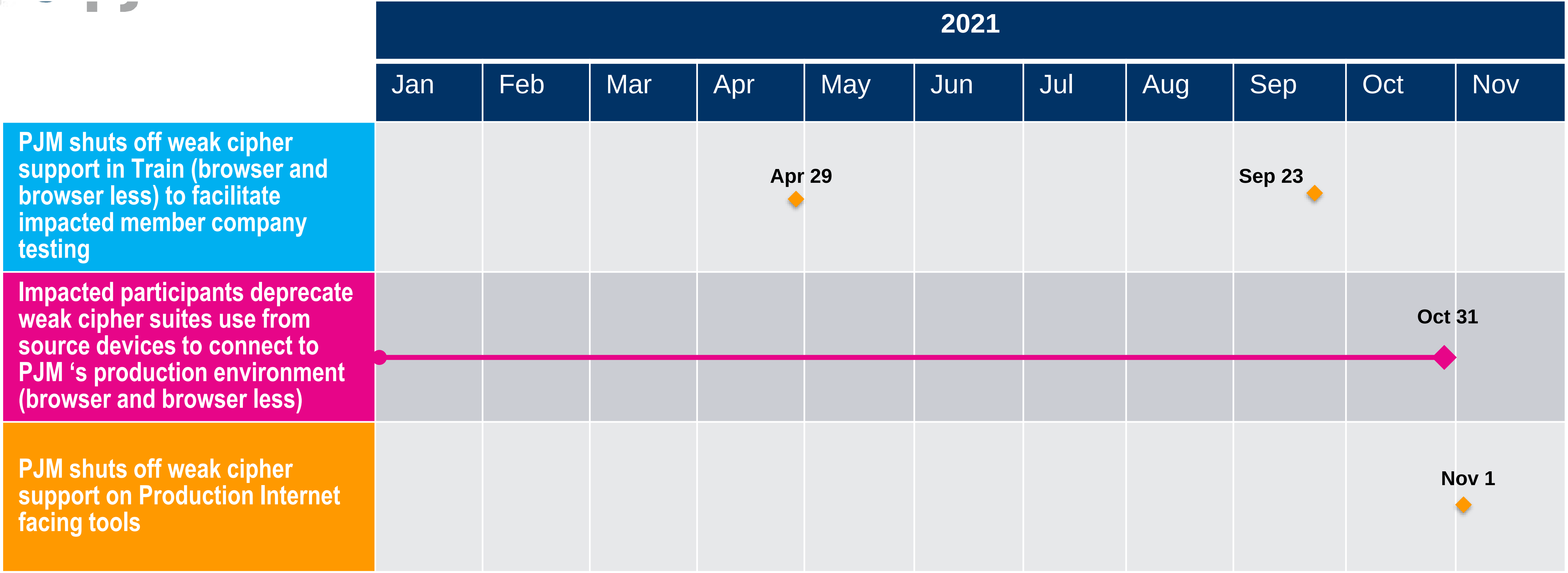
Sep 30

Legend

● Start Date

◆ End Date

Roadmap for Elimination of Weak Encryption



	2021										
	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov
PJM shuts off weak cipher support in Train (browser and browser less) to facilitate impacted member company testing				Apr 29 ◆					Sep 23 ◆		
Impacted participants deprecate weak cipher suites use from source devices to connect to PJM 's production environment (browser and browser less)	●									Oct 31 ◆	
PJM shuts off weak cipher support on Production Internet facing tools											Nov 1 ◆

Legend

● Start Date

◆ End Date

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
    - Additional TLS 1.2 ciphers were retired on September 23 2021
  - Browser and browser less support will stop on November 1 2021 in Production

- 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. The target date of completion is September 30 2021.

- Questions or feedback can be sent to: TechChangeForum@pjm.com.

Contact

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