Retiring use of Weak Encryption

January 20, 2021

Zeenath Fernandes

Sr Lead, Enterprise Information Security

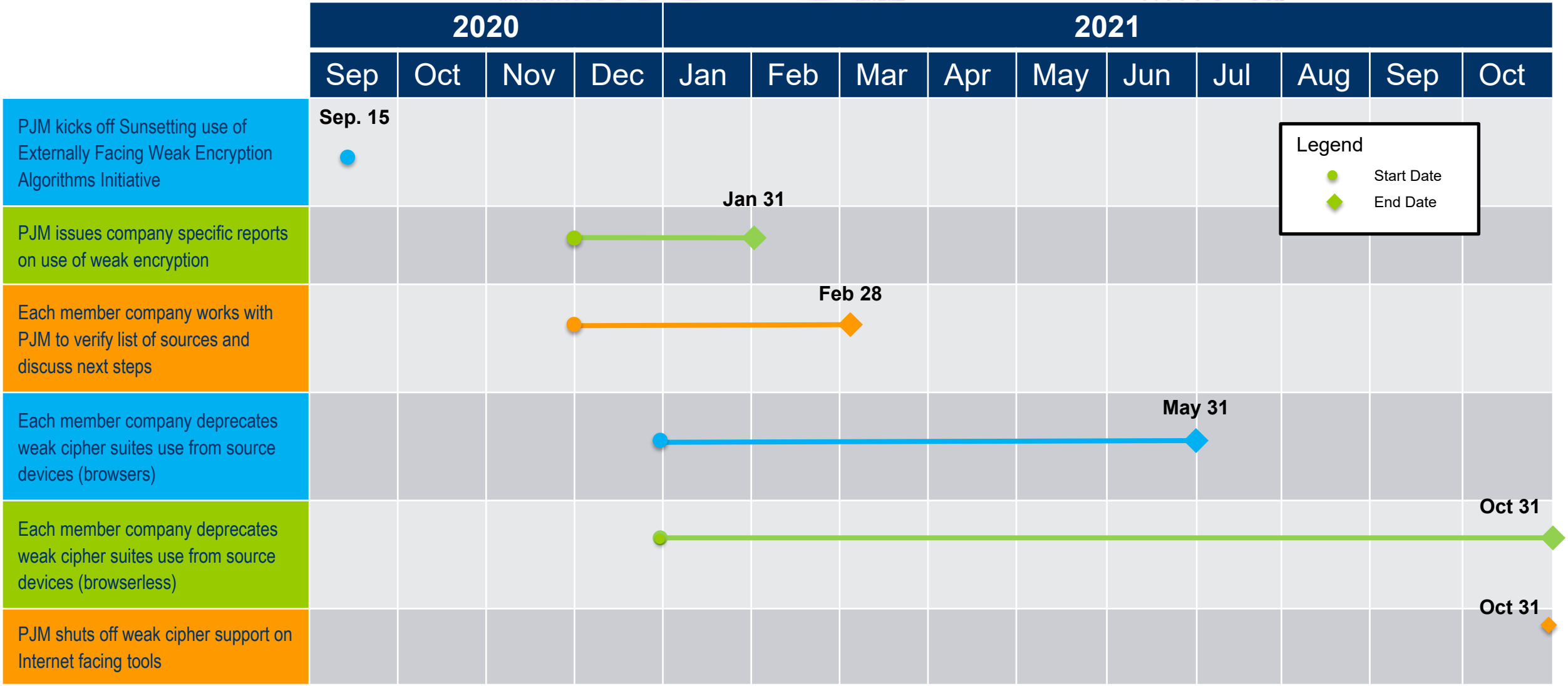
Revisions

- The process of issuing company specific reports on use of weak encryption will continue during month of January

Impact Details

Product - Action Required	Deadline	Who May Be Affected
PJM will supply a list of IP addresses/user ids using weak encryption ciphers/protocols by company. PJM requests that each company update the encryption on the source devices to use an acceptable level of encryption.	**May 31 2021 for browser based** **October 31 2021 for browserless systems**	• Any member who uses PJM's internet facing tools and uses 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



Background

- 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_* ciphers in TLS 1.2.
  - Members need to upgrade the encryption used on systems that connect to PJM externally facing systems.
  - Browser support will stop on May 31 2021
  - Support for browserless tools will stop on Oct 31 2021 as upgrading tools is expected to take more time
- These encryption mechanisms are no longer secure.

Details

- PJM will issue reports to each member negotiating weak encryption on PJM sites. The updated target date is January 31 2021.

- Members should contact PJM's member relations to discuss their next steps to stop using this encryption. The target date for this activity is February 28 2021.

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