

Retiring use of Weak Encryption

As of April 9, 2021 Zeenath Fernandes Sr. Lead, Enterprise Information Security

www.pjm.com | Public PJM © 2021



- Train Rollout Time Announcement
- Weak Encryption Remediation Guide



Impact Details

Product - Action Required

PJM will supply Weak Encryption Remediation Guide to the impacted member company. PJM requests that each company update the encryption on the source devices to use an acceptable level of encryption.

Deadline

April 29
10 a.m. to 4 p.m.
browser and browserless
systems

Production

November 1 browser and browserless systems

Who May Be Affected

- 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

2020					2021									
	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct
PJM kicks off Retiring use of Externally Facing Weak Encryption Algorithms Initiative	• Sep 15													
PJM issues company specific reports on use of weak encryption			•				Ма	31						
Impacted member company works with PJM to verify list of sources and discuss next steps									May	31				



Start Date

End Date



Roadmap for Elimination of Weak Encryption

2021

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





- 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_* 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 Nov 1 2021 in Production
- These encryption mechanisms are no longer secure.



- PJM will supply Weak Encryption Remediation Guide to the impacted member company. The target date of completion is April 15 2021.
- Impacted member company should contact PJM's <u>member relations</u> to verify list of sources and discuss next steps. The target date of completion is May 31 2021.
- Questions or feedback can be sent to: <u>TechChangeForum@pjm.com</u>.



Presenter:

Zeenath Fernandes

Zeenath.Fernandes@pjm.com

SME:

Zeenath Fernandes

Zeenath.Fernandes@pjm.com

Retiring use of Weak Encryption



Member Hotline

(610) 666 - 8980

(866) 400 - 8980

custsvc@pjm.com