

Retiring use of Weak Encryption

As of December 16, 2021

Zeenath Fernandes

Sr. Lead, Enterprise Information Security

- Rescheduled Production implementation for several applications
- Announced Production implementation for the Voting application

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. There is no impact if the company updates the encryption prior to Production deadline.</p>	<p>Production (browser and browserless systems)</p> <p>January 27 6 p.m. to 8 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: Voting</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. There is no impact if the company updates the encryption prior to Production deadline.</p>	<p>Production (browser and browserless systems)</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, ExSchedule, FTR Center, InSchedule, Markets Gateway, MSRS, OASIS, PJM.com, Planning Center, Power Meter, Resource Tracker, TO Connection, Tools Home</p>





Roadmap for Elimination of Weak Encryption

	2021									2022			
	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr
PJM shuts off weak cipher support in Train (browser and browser less)	Apr 29 ◆					Sep 23 ◆							
PJM shuts off weak cipher support on Production Internet facing tools								Phase 1 Nov 1 ◆	Phase 2 Dec 13 ◆	Phase 3 Jan 27 ◆			

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.
 - 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 Messages and Secure share
 - Browser and browser less support will stop on January 27 2021 in Voting
- These encryption mechanisms are no longer secure.

- 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.

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