



Security Update

Joe Callis
Manager, Cyber Security Operations
Center

Important Security Alerts

- **Entrust Breach:** Breach of a cyber security vendor led to customer data leakage.
- **Mantis Botnet DDOS Attacks:** Powerful botnet launched denial of service attacks.
- **CISA ICS Alerts:** 47 ICS/OT vulnerabilities announced in July.
- **DHS CSRB Log4j Report:** Review of the Log4j events.

PJM Actions

- Following DHS CISA shields up recommendations
- Blocking international and anonymized network traffic
- Prioritizing external vulnerability remediation
- Exercising incident response plans

Contact PJM

- To report unusual events, notify your normal PJM contacts.
- To report connectivity issues contact Member Relations.
- To report suspicious email, notify SecurityAlertTm@pjm.com.
- Share this info with your security team.

Transport Layer Security (TLS) securely transfers data between clients and servers.
TLS is used to secure data on websites (commonly known as HTTPS).

PJM has determined that use of older versions of TLS presents a security vulnerability.

TLS 1.0 and TLS 1.1 versions are no longer secure.

Interception/decryption of secured data is possible when depreciated versions are in use.

PJM is removing support for TLS 1.0 and TLS 1.1 and **will support only TLS 1.2 in production applications.**

- Support for TLS 1.0 and TLS 1.1 will be phased out, by application, according to the published schedule.
- Please review the Weak Encryption Remediation Guide on PJM.com > Markets & Operations > PJM Tools > PJM Security > [Weak Encryption Remediation Guide](#)
- Impacted companies should contact PJM's [Member Relations](#) to verify list of sources and discuss next steps.

PJM announced new target dates to move away from insecure TLS.
Please test in PJM Train environment and contact Member Relations if you have issues.

Product	Implementation Date
Data Viewer, eDART	Aug 01
Power Meter, InSchedule	Aug 10
FTR Center	Aug 11
Markets Gateway	Aug 15
MSRS, SSO, PJMeSuite	Aug 17

