



Security Update

Joe Callis
Manager, Cybersecurity Operations
Center

Important Security Alerts

- **Network access security:** [CISA guidance](#) on securing remote access to corporate networks.
- **Extremist groups use of AI:** [Threat groups are weaponizing and training AI](#) to aid in recruiting and messaging.
- **Threat actors posing as support:** Social engineering scammers [posing as CDK customer support](#).
- **Helpdesk social engineering campaign:** [EISAC memo](#) on social engineering tactics used against helpdesks.

Monitored Threats

- Exploitation of unpatched vulnerabilities
- Phishing and smishing attacks
- Distributed Denial of Service attacks
- Use of deepfake and Adaptive AI technology

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.

Presenter:
Joe Callis

Joseph.Callis@pjm.com

Security Update



Member Hotline

(610) 666 – 8980

(866) 400 – 8980

custsvc@pjm.com