Security Bulletin

TLP: WHITE

March 30, 2022

NPCC is publishing this security bulletin to engage and inform NPCC entities on aspects of Bulk Power System security and reliability.

Russian State-Sponsored Cyber Actors Access Network Misconfigured with Default MFA Protocols

This Joint Cybersecurity Advisory addresses exploitation of default MFA protocols and a known vulnerabilities to protect against:

- MFA configuration policies that allow “fail open” and re-enrollment scenarios.
- Exploitation of inactive accounts that are not disabled uniformly across the Active Directory and MFA systems.
- The exploitation of known vulnerabilities due to unpatched systems and applications.

The advisory lists threat actor activity, indicators of compromise, and mitigations.

CISA Resource: JCA Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and “PrintNightmare” Vulnerability

TLP: WHITE