



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

NPCC assumes no responsibility for any material, e.g., information, data, text, software, graphics et cetera, of computer “links” to sites hosted by third parties that are outside of NPCC’s control. NPCC does not endorse products, services, or information provided by third parties and shall not be responsible or liable, directly or indirectly, for any damage or loss caused or alleged to be caused by or in connection with, use or reliance on any content available on or through any third party site. Further, the inclusion of links to third party websites within this Security Bulletin does not imply that the owners of such third party websites have given permission for inclusion of these links, or otherwise sponsored or endorsed NPCC’s Security Bulletin.

NPCC is not responsible for the accessibility of third party websites via the Security Bulletin. Should you discover that a third party link on a Security Bulletin is broken, no longer pointing to the content so indicated on the Security Bulletin, or points to a third party website containing infringing content, malicious code, or any offensive, libelous, or otherwise illegal or inappropriate content, email: support@npcc.org. To ensure NPCC can quickly respond to the issue, your email should include the originating Security Bulletin, the linked page URL and a description of the content in question.