NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

Security Bulletin

TLP: WHITE

December 15, 2021

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

Zoho ManageEngine ServiceDesk Plus Vulnerability

On Thursday, December 2, 2021, the Cybersecurity & Infrastructure Security Agency (CISA) and Federal Bureau of Investigations (FBI) reported a new campaign targeting ManageEngine ServiceDesk Plus servers (on-premises) that are vulnerable to CVE-2021-44077.

CVE-2021-44077 is an unauthenticated remote code execution vulnerability in ManageEngine ServiceDesk Plus affecting all versions of ServiceDesk Plus up to, and including, version 11305. Following initial exploitation of CVE-2021-44077 on a targeted system, the threat actors have been observed uploading executable files and placing web shells that enable post-exploitation activities such as compromising administrator credentials, conducting lateral movement, and exfiltrating registry hives and Active Directory files.

Recommendations:

- Run the ManageEngine Exploit Detection Tool on ServiceDesk Plus Servers to discover any compromises in your environment
- Upgrade to the latest version using the appropriate migration path

Additional:

- The Electricity Information Sharing and Analysis Center (E-ISAC) also has more information on this topic.