



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.

**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](mailto: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.