



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

November 10, 2021

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

## 2021 CWE Most Important Hardware and Software Weaknesses

***Common Weakness Enumeration (CWE) has released the 2021 common hardware and software weaknesses to drive awareness of common weaknesses.***

The weaknesses can be found using the following links:

- [2021 CWE Most Important Hardware Weaknesses](#)
- [CWE Top 25 Most Dangerous Software Weaknesses](#)

*MITRE maintains the CWE web site with the support of the US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). "CWE Most Important Hardware Weaknesses is the first of its kind and the result of collaboration within the Hardware CWE Special Interest Group (SIG), a community forum for individuals representing organizations within hardware design, manufacturing, research, and security domains, as well as academia and government."*

Additional:

- The Electricity Information Sharing and Analysis Center (E-ISAC) has more information. E-ISAC access requires an ID If you need access, request an account (ID) at this link - <https://www.eisac.com/login>. If you have an ID, click this link to login - <https://www.eisac.com/login>.

**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.