



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

January 11, 2022

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

Apache Log4j Vulnerability Guidance

The Cybersecurity & Infrastructure Security Agency (CISA) and its partners issued guidance and multiple resources to mitigate the [CVE-2021-44228](#) (known as “Log4Shell”), [CVE-2021-45046](#), and [CVE-2021-45105](#) in Apache’s Log4j software library vulnerability. Log4j is broadly used in a variety of consumer and enterprise services, websites, and applications—as well as in operational technology products—to log security and performance information. The vulnerability allows an attacker who can control log messages or log message parameters to execute arbitrary code loaded from LDAP/RMI servers when message lookup substitution is enabled. The following mitigations are recommended:

- Discover all internet-facing assets that allow data inputs and use Log4j Java library anywhere in the stack.
- Update or isolate affected assets. Assume compromise, identify common post-exploit sources and activity, and hunt for signs of malicious activity.
- Monitor for odd traffic patterns (e.g., JNDI LDAP/RMI outbound traffic, DMZ systems initiating outbound connections).
- Follow CISA’s guidance on [Mitigating Log4Shell and Other Log4j-Related Vulnerabilities](#)
- Review CISA’s [Known Exploited Vulnerabilities Catalog](#) to see if your organization systems are affected.
- Recommend using GitHub’s [CERT/CC's CVE-2021-44228 scanner](#) to detect vulnerable applications.
- Monitor the [Apache Log4j Security Vulnerabilities Webpage](#) for updates and mitigation guidance.
- Review the [Electricity Information Sharing and Analysis Center \(E-ISAC\)](#) alerts related to Log4j.

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.