N A R U C

National Association of Regulatory Utility Commissioners

Issue Brief

Log4j Vulnerability

On December 9, 2021, news of a zero-day vulnerability referred to as Log4J began making headlines. The vulnerability lies in a piece of software called Log4J, part of a free, open-source software library managed by Apache. Log4J is used to log errors and other security information within applications developed for a wide variety of systems including IT, OT, and cloud services. Estimates suggest significant numbers of applications are vulnerable, including commercial and proprietary applications used in the energy sector. NIST rates the severity of the vulnerability a 10 out of 10.#

The Log4j vulnerability, if exploited, allows attackers to remotely execute malicious code and dig deeply into affected systems. On December 14, 2021, Microsoft reported groups originating from China, Iran, North Korea, and Turkey were actively attempting to exploit the vulnerability. Experts expect such activity to ramp up quickly.

DHS's Cybersecurity and Infrastructure Security Agency (CISA) suggests organizations take steps to close this easy-to-exploit vulnerability. These steps include identifying mission critical and internet-facing applications that run Log4j and upgrading them to the newest software version as well as enhancing security monitoring on devices running Log4j to identify potential attacks. CISA has developed a web page containing details of the Log4j vulnerability, mitigation measures, and links to other informative resources. The page also contains a list of third-party software known to include the Log4j vulnerability.

The Department of Energy is working with energy sector ISACs to ensure that actionable information is shared with industry. Further, DOE encourages affected entities to share information with ISACs regarding active exploitation attempts to aid in collaborative sector defense.

PUCs interested in gaining a better understanding of the Log4j vulnerability and the actions utilities are taking in response, might ask the following questions of their jurisdictional utilities:

- Have IT and OT applications been assessed for the Log4j vulnerability?
- Have patches been applied to vulnerable mission critical systems and internet-facing systems? If not, why not and what is the timeline for doing so?
- Are you monitoring vulnerable systems running Log4j for signs of exploitation? Has evidence been found?
- Are mechanisms in place to share actual or suspicious incidents with appropriate energy sector Information and Analysis Centers (ISAC)?
- Are you monitoring ISACs and CISA websites for updates on the vulnerability and applying additional mitigations as they become available?

December 20, 2021

Additional Resources:

https://www.cyberscoop.com/log4j-cisa-easterly-most-serious/

https://www.dragos.com/blog/industry-news/implications-of-log4j-vulnerability-for-ot-networks/

https://www.f5.com/labs/articles/threat-intelligence/explaining-the-widespread-log4j-vulnerability

https://www.mandiant.com/resources/log4shell-recommendations

https://www.zdnet.com/article/log4j-zero-day-flaw-what-you-need-to-know and-how-to-protect-yourself/

Acknowledgment
This material is based upon work supported by the Department of Energy under Award Number DE-CR0000009.