NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Industry Advisory

Apache Software Foundation Log4j, aka Log4Shell Vulnerability

Initial Distribution: December 14, 2021

NERC is aware of a critical remote code execution vulnerability in Apache Software Java logging library Log4j, CVE-2021-44228, which was announced December 9, 2021. Successful exploitation of this vulnerability may enable an adversary to install arbitrary malicious code leading to initial access to a targeted environment or full control over impacted system. Log4j is a commonly used, open-source, logging framework in Java developed by the Apache Foundation that is used in millions of applications around the world, including enterprise applications and numerous cloud services (such as Apple, Apache, Steam, Redis, ElasticSearch, and others). It is also used in open-source repositories and various industrial applications including Supervisory Control and Data Acquisition (SCADA), Energy Management Systems (EMS) and other operational technology (OT) environments. The U.S. government and security research teams have advised that the vulnerabilities are being actively exploited globally.

At this time, NERC is not aware of any known impacts to bulk power system (BPS) reliability or system outages related to the Log4j vulnerability. However, due to the pervasive use of Log4j, entities are likely exposed to this vulnerability and possible exploitation by advanced persistent and cyber-criminal adversaries. The E-ISAC issued an initial cyber bulletin raising industry awareness to this vulnerability on December 10, and an All-Points Bulletin (APB) 21-7 on December 12 to draw further attention and drive action.

Accordingly, the electricity industry is strongly urged to assess impact and immediately and apply the requisite patches to applications that leverage the Log4j Java library. In addition, registered entities are strongly encouraged to report any exploitation of these vulnerabilities to the E-ISAC, government agencies, and, if necessary, law enforcement to help the sector maintain situational awareness and coordinate response and mitigation activities. NERC also encourages registered entities to contact vendors in their supply chain to further assess exposure to their enterprise and operational technology environments.

Additional information can be found at:

- Apache Log4j Security Vulnerabilities
- CISA Apache Log4j Vulnerability Guidance
- E-ISAC All-Points Bulletin 21-07 - Active Exploitation of Log4j Java Vulnerability – Mitigate Now

Why am I receiving this? >>

[About NERC Alerts >>]

Status:	**No Reporting is Required – For Information Only**
🟩 🟨 🟥 ⬛	**PUBLIC (TLP Green):** No Restrictions. Will be posted to NERC's alert page. More on handling >>
Instructions:	NERC advisories are designed to improve reliability by sharing critical reliability information and are made available pursuant to Rule 810 of NERC's Rules of Procedure for use as your organization deems appropriate. **No response is necessary.** A NERC advisory is not the same as a Reliability Standard and your organization will not be subject to penalties for a failure to implement any recommendations or practices provided in this advisory. Additionally, issuance of this advisory does not lower or otherwise alter the requirements of any approved Reliability Standard, or excuse the prior failure to follow the practices discussed in the advisory if such failure constitutes a violation of a Reliability Standard.
Distribution:	**Initial Distribution:** Balancing Authority, Distribution Provider, Distribution Provider-UFLS, Frequency Response Sharing Group, Generator Owner, Generator Operator, Planning Authority, Reliability Coordinator, Resource Planner, Regulation Reserve Sharing Group, Reserve Sharing Group, Transmission Owner, Transmission Operator, Transmission Planner, and Transmission Service Provider **Who else will get this alert? >>** **What are my responsibilities? >>**
Primary Interest Groups:	Physical Security, Cyber Security - Control Systems, Cyber Security - Corporate Information Technology, System Operators, System Operators - System Protection, System Operations - Transmission Engineering, Generation Engineering, Transmission Planning, and Generation Operations
Advisory:	NERC is issuing this advisory to alert industry to the active exploitation of vulnerabilities impacting Apache's Log4j Java logging library. In addition, NERC strongly advises registered entities to review the information contained in the aforementioned CISA Log4j guidance site and Apache advisories, apply requisite patches as soon as possible and report any attempts to exploit the vulnerabilities along with indicators of compromise. A summary of recommended actions is detailed below: 1. Review the following: (1) Apache Log4j Security Vulnerabilities; (2) CISA Apache Log4j Vulnerability Guidance**;** (3) Log4Shell: RCE 0-day exploit found in log4j 2, a popular Java logging package; and (4) Guidance for

preventing, detecting, and hunting for CVE-2021-44228 Log4j 2 exploitation. In addition, if you are an E-ISAC member or are eligible to become one, please review the E-ISAC All-Points Bulletin 21-07 - Active Exploitation of Log4j Java Vulnerability – Mitigate Now.

Please also continue to visit the Cybersecurity and Infrastructure Security website to obtain the latest information.

2. Identify whether vulnerable applications exist in the environments that leverage the Log4j library. This may require coordination with software vendors and system integrators, as applicable. Additionally, monitor for malicious network connections that indicate reconnaissance scanning and possibly exploitation attempts. Some strings to look for in network connections are detailed in Microsoft's guidance for preventing, detecting, and hunting for CVE-2021-44228 Log4j 2 exploitation

3. If you have a vulnerable version(s) of Log4j Java logging library in your corporate and/or operational technology environments, immediately commence your patch management process and apply the appropriate approved patches as soon as possible. Note: Entities should continue to monitor their environments for malicious activity after the patches have been applied since adversaries may have introduced other malware or tools in order to maintain persistence.

4. Report any exploitation of these vulnerabilities to the E-ISAC (operations@eisac.com), U.S. Department of Homeland Security (DHS), U.S. Department of Energy, and if necessary, law enforcement as soon as possible.

Background:

On December 9, 2021, a new vulnerability in the popular Java logging library "log4j" was published on Twitter along with a link with proof of concept code found on the popular code sharing site Github. The "zero day" exploit was dubbed Log4Shell and allowed an unauthenticated remote adversary to install and download arbitrary code on the affected system. The Log4j vulnerability has been assigned CVE-2021-44228 with a criticality score of 10, which is the highest on the scale. Log4j is very broadly used in a variety of consumer and enterprise services, websites, and applications, as well as in operational technology products, to log system security and performance information. An unauthenticated remote actor could exploit this vulnerability to take control of an affected system. Active exploitation by advanced persistent and cybercriminal adversaries has been observed and reported by U.S. government and security research partners.

The E-ISAC strongly recommends patching these environments as soon as possible. The E-ISAC issued an All-Points Bulletin part of the Critical Broadcast Program regarding the observed exploits.

The E-ISAC has been advised that the vulnerabilities are being actively exploited and has requested that critical infrastructure sectors ensure entities are aware of the vulnerabilities and also advise them to apply the patches as soon as possible.

The E-ISAC will continue to provide updates and curated reporting on the on-premises Microsoft Exchange Vulnerability to vetted members of the electricity industry on its secure Portal. If your entity is not a member of the E-ISAC, please visit www.eisac.com to register for an account.

Contact:

For clarification or content-related questions, contact:
E-ISAC Operations (202) 790-6000 (24/7)
Email: operations@eisac.com

For login/account/registration issues, contact:
Bulk Power System Awareness Group
404-446-9797 | nerc.alert@nerc.net

Additional clarification or content-related questions can also be sent to the Cybersecurity and Infrastructure Security Agency

Alert ID: A-2021-12-14-01

You have received this message because you are listed as a primary compliance contact for your organization on the North American Electric Reliability Corporation's compliance registry. If you believe that you have received this message in error, please notify the sender immediately and delete or otherwise dispose of all occurrences or references to this email. If you have questions about your membership in this list, please contact NERC via email at nerc.alert@nerc.net.

North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560 | www.nerc.com