



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

December 23, 2021

SECURITY ADVISORY FOR POWER REACTORS, INCLUDING THOSE UNDER CONSTRUCTION; NONPOWER PRODUCTION AND UTILIZATION FACILITIES; DECOMMISSIONING REACTORS, INCLUDING THOSE THAT ARE PERMANENTLY DEFUELED BUT HAVE NOT TRANSITIONED TO DECOMMISSIONING; FUEL FABRICATION, ENRICHMENT, AND CONVERSION/DECONVERSION FACILITIES; INDEPENDENT SPENT FUEL STORAGE INSTALLATIONS; LICENSEES POSSESSING SPECIAL NUCLEAR MATERIAL UNDER TITLE 10 OF THE *CODE OF FEDERAL REGULATIONS* PART 70; LICENSEES REGULATED UNDER TITLE 10 OF THE *CODE OF FEDERAL REGULATIONS* PART 37; AND ALL RADIATION CONTROL PROGRAM DIRECTORS AND STATE LIAISON OFFICERS

SA 2021-13

SUBJECT: SITUATIONAL AWARENESS—APACHE LOG4J VULNERABILITY

On December 22, 2021, the U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) published Alert AA21-356A, "Mitigating Log4Shell and Other Log4j-Related Vulnerabilities" (<https://www.cisa.gov/uscert/ncas/alerts/aa21-356a>). As discussed in the alert, CISA and its partners are tracking and responding to active, widespread exploitation of critical remote code execution vulnerabilities in versions of Apache's Log4j software library, described in vulnerability reports CVE-2021-44228 (<https://nvd.nist.gov/vuln/detail/CVE-2021-44228>), CVE-2021-45046 (<https://nvd.nist.gov/vuln/detail/CVE-2021-45046>), and CVE-2021-45105 (<https://nvd.nist.gov/vuln/detail/CVE-2021-45105>). Log4j is very broadly used in a variety of consumer and enterprise services, Web sites, and applications, as well as in operational technology products, to log security and performance information. An unauthenticated remote actor could exploit this vulnerability to take control of a system if there is insufficient network segmentation to prevent connection to the internet or a pathway that allows remote system access via lateral movement from a compromised network. The U.S. Nuclear Regulatory Commission (NRC) is issuing this security advisory to provide situational awareness to its licensees and Agreement States.

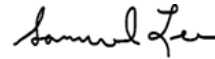
The NRC recommends that all licensees review the CISA alert and associated releases and take appropriate mitigative actions in accordance with licensee procedures and, where applicable, cyber security plans.

Suspicious activity reporting is important to the U.S. Government's security mission. The NRC encourages its licensees to remain vigilant and report cyber-related suspicious activity to CISA. Licensees subject to Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54, "Protection of digital computers, communication systems, and networks," are reminded of their obligation to report to the NRC certain cyber-related events under 10 CFR 73.77, "Cyber security event notifications."

If you have any questions concerning this advisory, contact the technical point of contact below.

Backfit Analysis Statement: This security advisory does not amend or impose new requirements or constitute a new or different regulatory staff position interpreting Commission rules and, therefore, does not constitute backfitting as defined in 10 CFR 50.109, "Backfitting," or 10 CFR 72.62, "Backfitting." Consequently, the staff did not perform a backfit analysis.

Paperwork Reduction Act Statement: This security advisory does not contain information collections and, therefore, is not subject to the requirements of the Paperwork Reduction Act of 1995 (Title 44 of the *United States Code*, Section 3501, et seq.).



Signed by Lee, Samuel
on 12/23/21

Approved by: _____

Samuel S. Lee, Acting Director
Division of Security Operations
Office of Nuclear Security
and Incident Response

Technical Contact: Brian Yip, NSIR
301-415-3154
brian.yip@nrc.gov

SA 2021-13 "Situational Awareness – Apache LOG4J Vulnerability" DATE December 23, 2021

DISTRIBUTION:

ADAMS Accession No.: Memo ML21356B494

* via email

| | | | | |
|--------|-----------------------------------|--------------------------|-----------------------|--------------------------|
| OFFICE | NSIR/DPCP/CSB | OGC/GCHA /AGCMLE/NLO* | NSIR | NMSS/DFM* |
| NAME | BYip <i>BY</i> | MLemoncelli <i>ML</i> | MGavrilas <i>MG</i> | SHelton <i>SH</i> |
| DATE | Dec 22, 2021 | Dec 22, 2021 | Dec 23, 2021 | Dec 23, 2021 |
| OFFICE | NSIR/DPCP/CSB | ADM/DRMA | NSIR/DSO/SOSB | OCIO/GEMSD /FLICB/ICT |
| NAME | BYip <i>BY</i> | JDougherty <i>JD</i> | JKeene <i>JK</i> | DCullison <i>DC</i> |
| DATE | Dec 22, 2021 | Dec 22, 2021 | Dec 22, 2021 | Dec 22, 2021 |
| OFFICE | NSIR | NMSS/MSST | NSIR/DSO | NSIR/DPR |
| NAME | SLee <i>SL</i> | KWilliams <i>KW</i> | SAtack <i>SA</i> | KBrock <i>KB</i> |
| DATE | Dec 22, 2021 | Dec 22, 2021 | Dec 22, 2021 | Dec 23, 2021 |
| OFFICE | NMSS/DFM | NRR/DORL | NSIR/DSO/ILTAB | NRR/DANU |
| NAME | CRegan <i>CR</i> | BPham <i>BP</i> | RRichardson <i>RR</i> | MShams <i>MS</i> |
| DATE | Dec 22, 2021 | Dec 23, 2021 | Dec 22, 2021 | Dec 23, 2021 |
| OFFICE | NRR/DANU | NMSS/DUWP | NSIR | |
| NAME | BSmith RCaldwell for <i>RC</i> | JMarshall <i>JM</i> | SLee <i>SL</i> | |
| DATE | Dec 22, 2021 | Dec 23, 2021 | Dec 23, 2021 | |

OFFICIAL RECORD COPY