**From:** AIG Cyber & Information Security Team

**To:** <affected team>

**Subject:** Security Advisory concerning NBN Connection Spring Framework 5.3.0

**Body:**

Hello NBN Team,

AIG Cyber & Information Security Team would like to inform you that a recent Spring Framework 5.3.0 vulnerability has been discovered in the security community that may affect NBN Connections.

[Log4Shell](https://nvd.nist.gov/vuln/detail/CVE-2021-44228), disclosed on December 10, 2021, is a remote code execution (RCE) vulnerability affecting Apache’s Log4j library, versions 2.0-beta9 to 2.14.1. The vulnerability exists in the action the Java Naming and Directory Interface (JNDI) takes to resolve variables. Affected versions of Log4j contain JNDI features—such as message lookup substitution—that do not protect against adversary-controlled Lightweight Directory Access Protocol (LDAP), Domain Name System (DNS), and other JNDI-related endpoints.

An adversary can exploit Log4Shell by submitting a specially crafted request to a vulnerable system that causes that system to execute arbitrary code. The request allows the adversary to take full control over the system. The adversary can then steal information, launch ransomware, or conduct other malicious activity.

Log4Shell and CVE-2021-45046—rated as critical vulnerabilities by Apache—are severe because Java is used extensively across IT and OT platforms, they are easy to exploit, and applying mitigations is resource intensive. Log4Shell is especially critical because it allows malicious actors to remotely run code on vulnerable networks and take full control of systems.

To address the breach, immediately identify, mitigate, and update affected products that use Log4j to the latest patched version. You should also inform your end users of products that contain these vulnerabilities and strongly urge them to prioritize software updates.

For any questions or issues, don’t hesitate to reach out to us.

Kind regards,

AIG Cyber & Information Security Team