December 16th, 2021 – Log4J

Impact of Apache Log4j Exploit on eni Products

After review, **eni** confirms that we do not utilize this library in any of our products or in the delivery of any of our products & services. This includes **NexGen EAP** mobile & web, **Balance*Benefits*** mobile and web, and all backend and supportive systems. We anticipate no impact.

We will continue to monitor and provide updates, if necessary.

Background

Recently, a new zero-day vulnerability in the popular Java library Apache Log4j (CVE-2021-44228) was uncovered. This vulnerability allows attackers to inject arbitrary code in Log4j versions 2.0-2.14.1. This Java library is widely used by multiple closed and open source projects.

This vulnerability is rated critical (CVSS severity level 10 out of 10), with immediate patching or mitigation recommended if affected, because it allows a possible Remote Code Execution when an attacker sends a malicious code string that gets logged by Log4j. That string allows the attacker to load Java onto a server and therefore take control.