DocStyle

December 20, 2021

MEMORANDUM

TO: ALL CLIENTS

Re: DocStyle Response to Apache Log4j Remote Code Execution Vulnerability

Dear Sir/Madam,

Log4j is an open-open source, Java-based logging utility that is widely deployed and used across a variety of enterprise applications, including many cloud services that utilize Apache web servers. The security vulnerability recently reported affects Java-based applications that use Log4j, of which we do not utilize during the development of our software.

The security of our products is a top priority and critical to protecting our customers. Our development teams can confirm that neither Apache, Log4j, or Java are currently utilized within any of our products, specifically DocStyle Convert (formerly DocStyle Desktop), the DocStyle Ribbon, NOVO Compare, PuR MetaData for Outlook, PuR MetaData Desktop, and the PuR MetaData Admin Panel.

We are reviewing the Apache Log4j Remote Code Execution vulnerabilities tracked in CVE-2021-44228 and CVE-2021-45046 and assessing any indirect impact it may pose to our products. We have reached out to our third-party providers, particularly production system applications and services, primary product licensing, development applications, and website hosting services to assess their status, threat readiness strategies, and mitigation techniques.

At this time, we have not detected any successful exploit attempts in our systems or solutions. Since this is an ongoing investigation, security updates or mitigation efforts will be communicated as they become available via https://www.docstyle.net/blog/. If you would like to be notified when we issue new guidance, we recommend that you subscribe to notifications on our website to be alerted of any changes to this or future advisories.

Sincerely,

Chris Cangero
Chief Executive Officer

☎ (305) 676-6600 ✉ info@docstyle.net 🌐 www.DocStyle.net
1200 Brickell Ave, Ste 1950, Miami, FL 33131