NYMBUS®

Dan Chemnitz
Chief Risk Officer
dchemnitz@nymbus.com
(m) 727.514.2324

December 17, 2021

In response to the recent Long4j security vulnerability (CVE-2021-44228) released on December 9, 2021, Nymbus would like to provide additional assurance regarding the protection of client-provided consumer Non-Public Information (NPI) data. The compromised products, with affected versions 2.12.1 and 2.13.0 through 2.15.0, were cited as being exploited by malicious persons with emergency actions required.

As part of Nymbus' incident response process, the Nymbus Security & Compliance Committee investigated the situation and has taken proper steps to mitigate the risk associated with the compromised versions.

Additionally, Nymbus confirmed that no consumer NPI data was compromised with all critical third-party service providers. The vast majority of vendors in question were not utilizing the compromised products. The few have ensured us that the software has been disabled or reverted to the last version of the software that was not impacted by this security incident.

Nymbus will continue to monitor the situation surrounding the zero-day vulnerability within Apache Log4j. Should any new information be presented, we will notify you accordingly.

Should you have any questions, please do not hesitate to contact me at the information listed above.

Regards,

Daniel S. Chemnitz
Chief Risk Officer

NYMBUS, INC.
76 S LAURA STREET, SUITE 1370
JACKSONVILLE, FL 32202

WWW.NYMBUS.COM
INFO@NYMBUS.COM