11215 N. Community House Rd, Suite 800 • Charlotte, NC 28277
800 733.8839
isolvedhcm.com

Notice to Customers & Partners – Apache Log4J / Log4Shell Vulnerability Statement

December 13, 2021

Dear Customers and Partners,

At isolved we understand the scope, severity and impact of the pervasive risks that cyber threats and human error present to our customers and partners, which is why we are updating you on our status regarding a recent cyber threat.

We have received several inquiries regarding the recently disclosed Apache Log4j / Log4Shell vulnerability. We want to proactively inform our customers and partners that we have no reason to believe that this vulnerability has or will impact isolved or our services.

The isolved Cybersecurity team has been monitoring this event since it was made public on December 10, 2021. Based on continuous monitoring and the fact that isolved does NOT leverage the open-source technology that this threat is targeting, we are confident that there is very-low to no risk to the isolved environment due to this vulnerability.

Please know that isolved will continue to monitor this event, stay actively engaged with our cybersecurity partners, and will remain diligent regarding any outside threats resulting from this vulnerability.

You can further review the isolved Trust Center – a single resource that provides necessary information to customers, partners and prospective customers about our governance, risk and compliance (GRC) processes and controls.

For the latest information and updates on this vulnerability and any recommended actions, please visit: Log4j – Apache Log4j Security Vulnerabilities

Thank you for being a trusted partner and customer of isolved,

Todd Atwood,
Chief Information Officer

Tom Watson,
Chief Information Security Officer