GENERAL ATOMICS

Supplier Announcement

Critical Alert: Apache Log4j Vulnerability

December 2021

Valued General Atomics Supplier,

As expressed in our Supplier Code of Conduct, General Atomics (GA) is committed to protecting and securing sensitive information and responding to the growing cyber threat posed to our customers and industry. As a Supplier to GA, you share in this commitment. Please read on regarding the recent discovery of a zero-day vulnerability in the Apache Log4j software library.

Apache Log4j is a Java-based open-source software library that is leveraged by many of the world's most popular software applications. The vulnerability could allow remote users to gain control of computers and systems or gain access for ransomware attacks with minimal effort.

On December 11, 2021, Director Jen Easterly of the Cybersecurity and Infrastructure Security Agency (CISA), released a statement and issued recommendations on the Log4j vulnerability. Her statement can be found here. Full CISA guidance for the Apache Log4j vulnerability can be found here.

Cybersecurity company Sophos has already detected hundreds of thousands of attempts since December 9 to exploit this vulnerability. The ubiquity of the Apache Log4j software library, the impact of the vulnerability, and the ease with which it can be exploited has security researchers classifying this vulnerability as "Severe".

Please review any contractual obligations, specifically those including DFARS 252.204-7012, to determine whether a cyber incident report to DC3 at https://dibnet.dod.mil is required. If you find it is necessary to file a report with DC3, please remember to inform your GA Purchasing Representative of the report number.

Additional information can be found on our website at the GA Procurement and the GA Cybersecurity websites.

Note: The information herein is provided for informational purposes only and does not constitute legal advice; nor does it imply a change in any existing Order.