LEWIS ROCA

LOG4SHELL VULNERABILITY POSES MASSIVE CYBERSECURITY THREAT

By John Gray, CIPP/US on 12/16/2021
Posted in Cybersecurity and Data Protection

A widely reported flaw in popular software known as Log4j poses a ***severe cybersecurity threat to organizations around the globe***, with hundreds of millions of devices at risk. Over the past week, government agencies, cybersecurity firms, and other members of the cybersecurity community have been scrambling to address the vulnerability, but reports indicate that numerous attacks have already been launched, and the impacts could be felt for some time.

Log4j is a free, open-source logging utility that has been built into innumerable applications and is used by almost every cloud service and enterprise network. The Log4j vulnerability, also known as Log4Shell, is relatively easy to exploit and allows threat actors to execute malicious code and seize control of affected systems. Reports indicate that the vulnerability has already been used to install cryptocurrency mining tools on hacked systems, to deploy ransomware, to exfiltrate data, and to insert "back doors" that may allow future access even after Log4Shell itself has been patched.

As a result, the U.S. Cybersecurity & Infrastructure Security Agency (CISA) and several of its Joint Cyber Defense Collaborative (JCDC) partners, including Cisco, IBM, and Microsoft, have issued (and are frequently updating their) guidance regarding this vulnerability. CISA has also ordered all federal civilian agencies to patch the vulnerability by no later than December 24, 2021, and various federal contractors, critical-infrastructure entities, and related vendors within the supply chain might need to establish similar compliance efforts in the near future.

Even in the absence of any mandatory patching requirements, we urge you to discuss Log4Shell ***as soon as possible*** with your information-technology and cybersecurity personnel and to follow CISA's guidance. In addition, please feel free to contact a member of our Data Protection and Cybersecurity Team if you would like to discuss this issue or if you have any other questions pertaining to data privacy or security.

Tags: Data Protection and Cybersecurity