BRACEWELL

INSIGHTS

Patch Up – Log4j and How to Avoid a Cybercrime Christmas

December 16, 2021

By: ***Seth D. DuCharme***

A vulnerability so dangerous that Cybersecurity and Infrastructure (CISA) Director Jen Easterly ***called*** it "one of the most serious [she's] seen in [her] entire career, if not the most serious" arrived just in time for the holidays. On December 10, 2021, CISA and the director of cybersecurity at the National Security Agency (NSA) began alerting the public of a critical vulnerability within the Apache Log4j Java logging framework. Civilian government agencies have been ***instructed*** to mitigate against the vulnerability by Christmas Eve, and companies should follow suit.

The Log4j vulnerability allows threat actors to remotely execute code both on-premises and within cloud-based application servers, thereby obtaining control of the impacted servers. CISA expects the vulnerability to affect hundreds of millions of devices. This is a widespread critical vulnerability and companies should quickly assess whether, and to what extent, they or their service providers are using Log4j.

Immediate Recommendations

- Immediately upgrade all versions of Apache Log4j to 2.15.0.
- Ask your service providers whether their products or environment use Log4j, and if so, whether they have patched to the latest version. Helpfully, CISA sponsors a community-sourced GitHub ***repository*** with a list of software related to the vulnerability as a reference guide.
- Confirm your security operations are monitoring internet-facing systems for indicators of compromise.
- Review your incident response plan and ensure all response team information is up to date.
- If your company is involved in an acquisition, discuss the security steps taken within the target company to address the Log4j vulnerability.

The versatility of this vulnerability has already ***attracted*** the attention of malicious nation-state actors. For example, government-affiliated cybercriminals in Iran and China have a "***wish list***" (no holiday pun intended) of entities that they are aggressively targeting with the Log4j

vulnerability. Due to this malicious nation-state activity, if your company experiences a ransomware attack related to the Log4j vulnerability, it is particularly important to pay attention to potential sanctions-related ***issues***.

Companies with additional questions about the Log4j vulnerability and its potential impact on technical threats and potential regulatory scrutiny or commercial liability are encouraged to contact counsel.