Log4j
HHS 405(d) Program SBAR Brief
December 17, 2021

The 405(d) **S**ituation, **B**ackground, **A**ssessment, **R**ecommendation (SBAR) is an HPH focused review of active cyber intelligence and alerts from across federal agencies. Mandated by the Cybersecurity Act of 2015 with the goal of aligning industry security approaches, the 405(d) **SBARs**, backed with the knowledge and expertise of HHS and the 405(d) Task Group, provide the HPH sector with a clear HPH focused understanding, assessment, and recommended mitigations that HPH organizations can apply against these active cyber incidents.

A concise statement of the problem

SITUATION: A potentially catastrophic vulnerability has recently been identified that applies to a common application called Log4j. This vulnerability is found in products that have Java based software installed. The software was created by The Apache Software Foundation and is widely used in applications, inclusive of Linux and Windows operating systems. The exploitation allows the execution of any code which could result in compromise of the server, download of malicious binaries, or propagation of further attacks such as ransomware or a zero-day attack. Healthcare and Public Health (HPH) organizations are being urged to review the recently released Apache security patch with their security team and take immediate action to secure their organization and protect their patients. The link to the patch can be found here: Apache Log4j Vulnerability Guidance | CISA. Also, continue to check for the latest updates as there are still many unknown implications of this vulnerability. The patch may not supply a fix for all organizations because of legacy systems that may be present in their network.[1] There are other security precautions that can be put in place to secure your organization. Continue reading for additional tools and resources.

Pertinent and brief information related to the situation

BACKGROUND: This tool is used universally between developers and vendor solutions for enabling logging features in their applications. Log4j is an open source tool, which means that it is easily available and free to use. It is often downloaded by any size organization to assist with user error log information, such as how many times an employee incorrectly enters their password when logging into their computer.

This is a commonly used vendor product and IT solution. It can be susceptible to hackers who can use this access to perpetrate further attacks against the organization, such as deploying malware, downloading more attack tools, and pivoting into the broader network.

Analysis and considerations of options—what we found and think

ASSESSMENT: The popularity and accessibility of the Log4j software makes it a potential risk to all healthcare organizations regardless of size. This vulnerability is becoming more widespread every day. At this time, the true impact of this vulnerability is unknown because the various ways of exploitation are still being identified. It is estimated that this vulnerability could potentially affect hundreds of millions of devices, networks, and/or software platforms.

Healthcare organizations are dependent on readily available devices and software that are vendor supplied and connected to an external network to operate. These complex and interconnected devices affect patient safety and privacy. They represent potential attack vectors across an organization like medical equipment such as bedside monitors that monitor vital signs during an inpatient stay. Or, they may be more complicated, like infusion pumps that deliver specialized therapies and require continual drug library updates. If an attacker gained access to the network through a vulnerability such as Log4j, they would be able to gain control of the software and could potentially disconnect devices from the network, therefore, causing a disruption to daily procedures and putting patient safety at risk.

Many mainstream and well-known organizations, including cloud services, are already utilizing the Log4j software and may be vulnerable. This includes cloud applications that medical organizations utilize for Electronic Health Records (EHR) services and outsourced security services such as Software as a Service (SaaS). For an updated list of vendors/products that are affected, please visit: https://github.com/cisagov/log4j-affected-db

Recommended/ requested action—what we want you to do

RECOMMENDATION: Work closely with your third-party service provider, vendors, or outsourced security services. Organize a response to determine your exposure to this vulnerability. Visit the link below on CISA.gov for detailed guidance. Below are a few additional actions to consider:

1. **Block inbound Internet based access to vulnerable products until a patch or mitigation can be put into place.** It is important to secure entry points to your network and enforce network traffic restrictions. These restrictions may apply to applications and websites, as well as to users in the form of allowing access only to tools that they need to complete their job duties. "Restricting access to personal websites will limit exposure to browser add-ons or extensions, in turn reducing the risk of cyberattacks."[2]
2. **This will provide a barrier between trusted and untrusted network traffic.** Always remember to update firewall security rules when new vulnerabilities are identified to limit any cyber-attacks from spreading across your network. "Most modern firewall technologies that are used to segment your network include an intrusion prevention systems (IPS) component. Implementing IPS and configuring them to update automatically reduces your organization's vulnerability to known types of cyber-attacks."[3]
3. **Conduct vulnerability scans against your environment to discover vulnerable assets.** Be sure to complete web application scanning of internet-facing webservers, such as web-based patient portals. If possible, invest in specialized vulnerability scanners that can "interrogate running web applications to identify vulnerabilities in the applications design."[4]
4. **Apply the Apache patch.** Visit the CISA website for additional guidance on applying the most current patch available. Always test any patches in a test environment before applying to your production network. Only "implement patches that are distributed by the vendor community, if patching is not automatic."[4]
5. **If you cannot apply the patch,** decommission the solution if no longer needed, or research other available tools that provide the same log feature.
6. **Stand up your incident response functions and discover all assets that are vulnerable.** Track in a central repository and apply patches as necessary. Confirm that your incident response plan has been implemented. Ensure "compliance with the plan's elements. At minimum, your plan should describe steps to be followed in the event of malware downloaded on a computer or upon receipt of a phishing attack."[6]
7. **Work with your security POC to monitor inbound attacks against your perimeter.**
8. **Review your software inventory and work with your vendor to determine if the asset is vulnerable.** Incorporate good cybersecurity practices into your asset procurement process. Instruct the vendor to provide you with proof that they have tested your environment for the Log4j vulnerability. Ensure they are completing the procurement life cycle to maintain data accuracy and integrity. "For each asset, the lifecycle includes procurement, deployment, maintenance, and decommissioning."[5] For more information, see CISA's Log4j Vulnerability Guidance on github.

Additional Resources:

- Apache Log4j Patch
- CISA: Apache Releases Log4j Version 2.15.0 to Address Critical RCE Vulnerability Under Exploitation
- NIST: Vulnerability Change Records for CVE-2021-44228
- HC3: Log4j Sector Alert
- CISA Log4j (CVE-2021-44228) Vulnerability Guidance
- HHS 405(d) Program

Sources:

1. 'The Internet Is on Fire,' *Wired*
2. HICP Technical Volume 1: 6.S.A, p19
3. HICP Technical Volume 1: 6.S.C, p20
4. HICP Technical Volume 1: 7.S.A, p21
5. HICP Technical Volume 2: CSP 5, p52
6. HICP Technical Volume 1: 8.S.A, p22