CROWDSTRIKE SERVICES

CROWDSTRIKE

CROWDSTRIKE SERVICES

LOG4J REMOTE CODE EXECUTION VULNERABILITY

QUICK REFERENCE GUIDE

Version 8
Dated: December 29, 2021

Background

Between late November and early December 2021, a critical vulnerability impacting the Log4j2 library was reported, resulting in several fixes and code revisions from the vendor[1]. Log4j2 is an open-source, Java-based logging framework used in numerous Apache frameworks (including Struts2, Solr, Druid, and Flink)[2]. As of December 9, 2021, CrowdStrike Falcon Overwatch and external sources have confirmed active exploitation of this vulnerability in the wild.

This critical vulnerability, tracked as CVE-2021-44228 (aka "Log4Shell"), impacts all versions of Log4j2 from 2.0-beta9 to 2.14.1. Exploitation of the Log4j2 vulnerability allows Remote Code Execution (RCE)[3].

On December 13, 2021, Apache released Log4j versions 2.16.0 and 2.12.2 in a security update to address the CVE-2021-45046 vulnerability[4]. A remote attacker can exploit this second Log4j vulnerability to cause a denial-of-service (DOS) condition in certain non-default configurations in all versions from 2.0-beta9 through 2.12.1 and 2.13.0 through 2.15.0.

On December 18, 2021, Apache released Log4j version 2.17.0 in a security update to address the CVE-2021-45105 vulnerability[5]. Apache Log4j2 versions 2.0-alpha1 through 2.16.0 did not protect from uncontrolled recursion from self-referential lookups. This allows an attacker with control over Thread Context Map data to cause a denial of service when a crafted string is interpreted. On December 21, 2021, patches were released to address these vulnerabilities in Log4j version 2.3.1 for Java 6 and version 2.12.3 for Java 7, in addition to the previously updated 2.17.0 for Java 8[6][7].

On December 28, 2021, an additional vulnerability tracked as CVE-2021-44832 was announced, which impacts Log4j versions 2.0-beta7 through 2.17.0[8]. These releases are vulnerable to a RCE attack where an attacker with permission to modify the logging configuration file can construct a malicious configuration using a JDBC Appender with a data source referencing a JNDI URI which can execute remote code. Log4j2 version 2.17.1 was released to address this issue for Java 8 or later[9]. Additionally, on December 29, 2021, Apache released additional patched versions of Log4j for Java 7 (2.12.4) and Java 6 (2.3.2)[10] [11].

[1] https://www.crowdstrike.com/blog/log4j2-vulnerability-analysis-and-mitigation-recommendations/

[2] https://arstechnica.com/information-technology/2021/12/minecraft-and-other-apps-face-serious-threat-from-new-code-execution-bug/

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

[4] https://nvd.nist.gov/vuln/detail/CVE-2021-45046

[5] https://nvd.nist.gov/vuln/detail/CVE-2021-45105

[6] https://logging.apache.org/log4j/log4j-2.3.1/download.html

[7] https://logging.apache.org/log4j/log4j-2.12.3/download.html

[8] https://nvd.nist.gov/vuln/detail/CVE-2021-44832

[9] https://logging.apache.org/log4j/2.x/download.html

[10] https://logging.apache.org/log4j/log4j-2.12.4/download.html

[11] https://logging.apache.org/log4j/log4j-2.3.2/download.html

Users of Apache Log4j are advised to upgrade to version 2.17.1, where feasible. It is imperative that organizations patch vulnerable infrastructure as soon as possible. As with any RCE vulnerability on largely public-facing services, denying unknown actors with unknown intentions the ability to repeatedly remotely execute code and attempt to evade security tooling is paramount. The effort required for exploitation of these vulnerabilities is trivial.

Impact

The Log4j2 library is often included or bundled with third-party software packages and is very commonly used in conjunction with Apache Struts. When exploited, the Log4j2 vulnerability will allow RCE - this presents a high-risk to organizations, especially for software packages such as Apache Struts that are typically internet-facing[12.] Similar to other high-profile vulnerabilities such as *Heartbleed* and *Shellshock*, there will potentially be an increasing number of vulnerable products discovered in the weeks to come.

Currently, CrowdStrike is observing a high volume of unknown actors actively scanning and attempting exploitation of the vulnerabilities. Due to the ease of exploitation and the breadth of applicability, ransomware and state-sponsored actors may also begin to leverage this vulnerability for their operations. As of December 12, 2021, CrowdStrike has already identified exploitation of the Log4j2 vulnerability that resembles targeted intrusions consistent with advanced attackers, such as deploying web shells and conducting lateral movement.

Recommendations

If you believe you may be impacted by CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, and/or CVE-2021-44832, assess the use of Log4j within your environments and consider the following:

- Patch vulnerable infrastructure by implementing one of the mitigation techniques below:
  - Upgrading to Log4j release version 2.17.1 for Java 8 or later, version 2.12.4 for Java 7, and version 2.3.2 for Java 6 users, which fixes this issue by limiting JNDI data source names to the java protocol. The JDBC Appender will use JndiManager and will require the log4j2.enableJndiJdbc system property to contain a value of true for JNDI to be enabled.
  - In prior releases, confirm that if the JDBC Appender is being used, that it is not configured to use any protocol other than java.
- Affected organizations that have already upgraded to earlier versions will need to upgrade to the latest available patch version in order to be protected against all currently known vulnerabilities.
- Preserve digital evidence as much as possible prior to performing any remediation actions such as patching, rebooting, shutdown, etc. It is recommended that you preserve memory and disk evidence for potentially affected systems.
- Ensure your CrowdStrike Falcon prevention policies are configured per our best practices
- Log4j2, as a library, may be embedded as a component of a wide range of vendor products/applications and the list of impacted vendors continues to grow (e.g., Cisco,

[12] https://supportportal.crowdstrike.com/s/article/Tech-Alert-CVE-2021-44228-aka-Log4Shell

Citrix, VMware, etc.)[13][14][15]. Follow vendor-specific guidance for mitigation, patch, and/or update procedures.

- Apache has released specific mitigation recommendations in the event Log4j2 cannot be patched. If you have implementations of Log4j2 that cannot be patched, it is recommended that organizations implement the mitigations noted on the following Apache advisory page: https://logging.apache.org/log4j/2.x/security.html.
- Identify critical applications/services and remain up to date with vendor-specific recommendations as the situation develops.

Testing Best Practices

A common approach to identifying vulnerable systems is to send Proof-of-Concept (PoC) payloads that will trigger a callout and indicate the vulnerability is present. In the case of CVE-2021-44228, the endpoint receiving the payload may not be the host that runs the PoC code, which can lead to difficulties identifying the vulnerable system. Some suggestions when running PoC exploits for identification of vulnerable systems are as follows:

- Ensure the payload is clearly marked "INTERNAL_TESTING" or has some other unique indicator to prevent incident response teams from investigating the activity as malicious.
- Encode information about the endpoint being tested so it can be traced back to the initial request. For example, if a request is being sent to http[:]//testing.url/login, encode that string as Base64 and include it somewhere in the payload.
- Utilize environment variables that are interpolated on the vulnerable host that is executing the payload. For example, including ${env:HOST} in the payload will include that variable, if it is set, in the response callout.

Additional Resources

For Falcon Customers

- Trending Threats & Vulnerabilities: Log4Shell
    - Falcon Dashboards
    - Knowledge Articles
    - Falcon Intel Briefs
- CrowdStrike Tech Alert
- CSA-211096
- CSA-211099
- CSA-211103

For Non-Falcon Customers

- CrowdStrike Vulnerability Learning Center
- CrowdStrike Archive Scan Tool (CAST)
- National Vulnerability Database(NVD) Common Vulnerabilities and Exposures(CVE)
- Apache Notification
- LunaSec Write-up

[13] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-httpd-2.4.49-VWL69sWQ
[14] https://support.citrix.com/article/CTX335705
[15] https://www.vmware.com/security/advisories/VMSA-2021-0028.html

CROWDSTRIKE SERVICES

If you require additional assistance, please reach out to CrowdStrike's support team at support@crowdstrike.com or contact us via phone:

Americas/Canada	+1 888 512 8906
UK/Ireland	+44(0) 118 453 0400
Australia/New Zealand/APAC	(+61) 1300 245 584
Middle East/Turkey/Africa	+9714 429 5829

If further help is required and you would like to engage CrowdStrike's Incident Response team, please contact Professional Services by completing the form on https://www.crowdstrike.com/experienced-a-breach or contact us via phone:

Americas/Canada	+1 855 276 9347
UK/Ireland	+44 800 0487187
France	+33 801840073
Germany	+49 (0800) 3252669
Australia	+61 1800 290 853
Japan	+81 800 170 5401
India	+91 1800 040 3447
Saudi Arabia	+966 8008803012
UAE	+971 8000320534
Qatar	+974 800101302

Customers with an active CrowdStrike Services retainer should notify the Services team in accordance with the process outlined in your retainer agreement.

CROWDSTRIKE SERVICES

WE STOP BREACHES

QUICK REFERENCE GUIDE