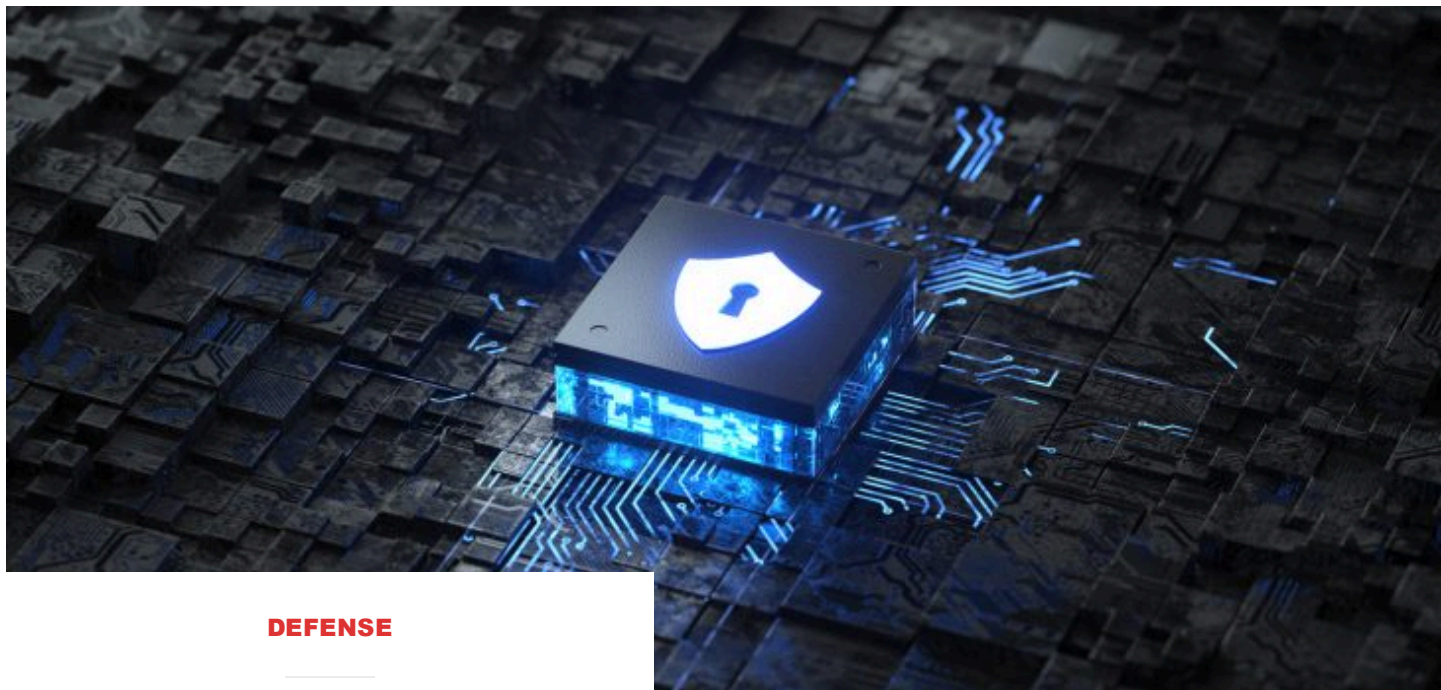


# PWNDEFEND



## TLDR

Go and run this on the connection servers:

<https://github.com/mr-r3b00t/CVE-2021-44228>




It's crude so also look for the modified timestamps, recent unexpected blast service restarts and if you have process logging go and check for suspicious child processes over the period. Once you have checked, run a backup, then if they aren't patched, patch the servers! (i know patching isn't as simple as just patch!)

## Introduction

In Decemebr a critical vulnerability (created by a feature request) in Log4J was discovered (named Log4Shell), unveiling the reality that an enormous amount of products may be vulnrable to a relativley simple remote code

execution vulnerability (which includes a huge range of internet facing systems, such as vmware horizon).

Response Matrix:

Product	Version	Running On	CVE Identifier	CVSS v3	Severity	Fixed Version	Workarounds	Additional Documentation
VMware Horizon	8.x, 7.x	Any	CVE-2021-44228, CVE-2021-45046	10.0, 9.0	Critical 	2111, 7.13.1, 7.10.3	KB87073	None
VMware vCenter Server	7.x, 6.7.x, 6.5.x	Virtual Appliance	CVE-2021-44228, CVE-2021-45046	10.0, 9.0	Critical 	Patch Pending	KB87081	None
VMware vCenter Server	6.7.x, 6.5.x	Windows	CVE-2021-44228, CVE-2021-45046	10.0, 9.0	Critical 	Patch Pending	KB87096	None

I'm going to be vague here on purpose, mainly because I'm not omnipotent and the scale of the challenge here is significantly large that it's subject to change. The constant phrase with log4shell is "dynamic and evolving". To be blunt, the intel we are getting is changing very rapidly from both a threat and vulnerability perspective.

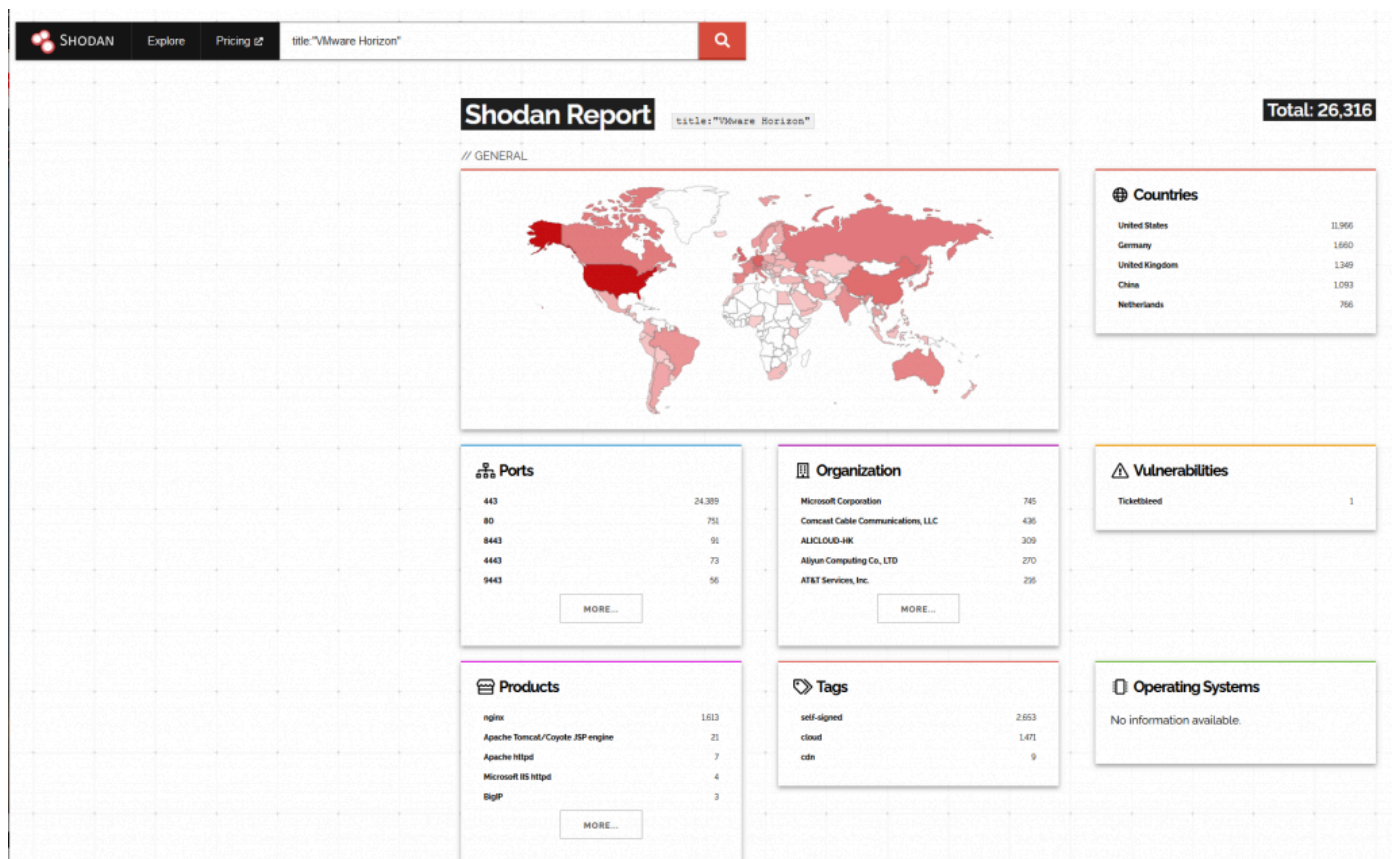
The Log4J scenario to some is a non event, but when we look at this at scale and when we look at certainly technology stacks it has really serious potential for negative impact. Public facing services such as:

- VMware Horizon
- VMware Vcenter (don't ask why people put this online but it seems lots them do!)
- VMware Worksapce One
- Mobile Iron
- Unifi
- Citrix XenMobile
- Fidelis commandpost

For a list of currently known affected products please see:

<https://github.com/cisagov/log4j-affected-db/blob/develop/SOFTWARE-LIST.md>

## Vmware Horizon World View



As you can see there are potentially one or two horizon services exposed! (let alone vcenters)

## Timeline

Early December ~9th December 2021 the vulnerability was publicly disclosed

12/12/2021 – VMware publishes KB to partially address the vulnerability (workaround) on VMware Horizon (<https://kb.vmware.com/s/article/87081>) – this has been updated all through December

12/12/2021 – VMware publishes advisory <https://www.vmware.com/security/advisories/VMSA-2021-0028.html>

13/12/2021 – UK NCSC Advisory <https://www.ncsc.gov.uk/news/apache-log4j-vulnerability>

16/12/2021 – VMware Horizon “Fixed” Builds released <https://kb.vmware.com/s/article/87073>

17/12/2021 – VMware Horizon releases new builds for some version of Horizon  
<https://kb.vmware.com/s/article/87073>

23/12/2021 – Exploitation of VMware Horizon discovered in the wild (across geos from the CTI we have)

24/12/2021 Active in the wild exploitation of vmware horizon

25/12/2021 – Active in the wild exploitation of vmware horizon

03/01/2022 – Microsoft Update <https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/>

05/01/2022 – mRr3b00t publishes initial backdoor detection script in Github (<https://github.com/mr-r3b00t/CVE-2021-44228>)

05/01/2022 – NHSD Publishes <https://digital.nhs.uk/cyber-alerts/2022/cc-4002>

07/01/222 – PwnDefend Post with detection examples

14/01/2022 – Increased detection activity noted  
(<https://twitter.com/TheDFIRReport/status/1482078434327244805>)

## Detections

The Log4J Payloads into the web services aren't so easy to detect. They will basically look like standard traffic and without full packet captures and TLS inspection you almost certainly (based on research in the lab) see the malicious payloads.

You will in the logs however see error events, so there will be a ton of logs in the UAGs and Connection server logs that occur when a failed attempt to exploit log4j occurs.

In short (but subject to loads of configuration and environmental variance) we have found:

In the standard vmware logs you will largely not see exploitation. You will likely see failed exploitation attempts. There are some logs which show a connection but the metadata is limited. E.g. it will hav source IP, time and path however depending upon your load balancer configurations you may just see the UAG connect to the Connection server and access a path used in normal operations.

## Process Logging

Process logging in sysmon will show execution of both log4j when the java child processes are spawned. It is however possible that a malicious class load could run in memory and use native win32 APIs and NOT spawn a child process (we haven't tested that yet).

# Backdoor

Backdoors can be detected by looking for file modifications here: (default path) C:\Program Files\VMware\VMware View\Server\appblastgateway\lib

The script I knocked up is crude but will detect the activity seen recently in the wild.

<https://github.com/mr-r3b00t/CVE-2021-44228>

you can also use a PowerShell one liner:

```
$path=gwmi win32_service|?{$_.Name -like "*VMBlastSG*"}|%{$_.PathName -replace "nssm.exe","lib\absg-worker.js"};$path = $path -replace '"','' ;Get-Content $path|Select-String "req.headers\[\'data\'\"]"
```

you can also look at the modification stamps:

```
$path=gwmi win32_service|?{$_.Name -like "*VMBlastSG*"}|%{$_.PathName -replace "nssm.exe","lib\"};$path = $path -replace '"','' ;dir $path
```

In our testing we have found the stamps on all files should be the same, a file with a different date has likely been modified in a suspicious manner.

# Microsoft Defender for Endpoint

These queries can be narrowed down and you should filter these onto your specific Horizon infrastructure, so they are examples for guidance, you will likely need to do some tweaks and mods:

Log4J (TCP 443) child process creations (check for benign normal child processes)

## Look for evil using powershell etc.

```
DeviceProcessEvents
| where DeviceName has_any("horizon-con-001") //connection server name
| where InitiatingProcessParentFileName == @"ws_TomcatService.exe"
| order by Timestamp desc
```

## Check for backdoors being created by powershell for file modification events:

```
DeviceFileEvents
| where FileName has_any("absg")
| where FolderPath has_any("appblastgateway")
| where ActionType == "FileModified"
| where InitiatingProcessCommandLine has_any("powershell")
| order by Timestamp desc
```

## Check network connections from ws\_TomcatService.exe






```
DeviceNetworkEvents
| where DeviceName has_any("horizon-con-001")
| where InitiatingProcessCommandLine == @"""ws_TomcatService.exe"" -SCMStartup TomcatService"
| where RemoteIP != @"127.0.0.1"
| where ActionType == @"ConnectionSuccess"
```

Please note that in our lab testing we do not see all the connections in MDE. So this data is deemed to be incomplete:

RemotePort
1387
8009
1387
1389

## Backdoor Usage (TCP 8443)

The backdoor seen is in abs-g-worker.js (but remember the log4j rce here could be used in many many ways:

 abs-g.js	06/02/2020 19:38	JavaScript File	1 KB
 abs-g-config.js	06/02/2020 19:38	JavaScript File	30 KB
 abs-g-master.js	06/02/2020 19:38	JavaScript File	58 KB
 abs-g-udp.js	06/02/2020 19:38	JavaScript File	50 KB
 abs-g-worker.js	07/01/2022 16:13	JavaScript File	44 KB

You can see in this instance the modified date looking quite out of place against the files peers.

```
DeviceProcessEvents
| where DeviceName has_any("horizon-con-001") //connection server name
| where InitiatingProcessParentFileName == @"node.exe"
| order by Timestamp desc
```

In our limited testing we can see backdoor usage which spawns child processes from node.exe

FileName
ipconfig.exe
cmd.exe
ipconfig.exe
cmd.exe
ipconfig.exe
cmd.exe
ipconfig.exe
cmd.exe
ipconfig.exe
cmd.exe
ipconfig.exe
cmd.exe
ipconfig.exe
cmd.exe
ipconfig.exe
cmd.exe

We should also note both in the lab and in the wild we have seen the following:

```
[2022-01-06 08:34:44.581] [DEBUG] 8072 [absg-worker] - Listener started
[2022-01-06 08:35:46.593] [ERROR] 8072 [absg-worker] - Missing route token in request /
[2022-01-06 08:50:08.608] [INFO] 8600 [absg-master] - Node.js version: v8.16.2
```

A very simmilar message is logged on the connection server when a failed backdoor attempt is made. This can be found in:

C:\ProgramData\VMware\VDM\logs\Blast Secure Gateway\absg.log



# Service Restart Events

If a backdoor is installed to the BLAST service then you will likely see the service restart at an unexpected time:

```
Get-EventLog -LogName "System" -Source "Service Control Manager" -EntryType  
e "Information" -Message "*VMWARE*running*"
```

that will list all the service restarts in the SYSTEM log on the Connection Server/s or we can just grab the blast service:

```
Get-EventLog -LogName "System" -Source "Service Control Manager" -EntryType  
e "Information" -Message "*Horizon View Blast Secure Gateway*running*"
```

## Useful logs

- If WAF is inline WAF logs would be useful
- SYSMON (process launches, dns events)
- EDR Process Logging (process launches, file writes)
- Load Balancer HTTP Traffic Logs
- Connection Server debug logs and blast logs
- Firewall (ingress and egress traffic logs)
- UAG blast logs
- DNS Logs (however we are seeing threat actors use IP addresses for the LDAP call backs)

## Vmware Horizon Log Levels

In the lab we observed the following:

- By default the UAG log level was set to INFO
- Debug logging is set on the connection server (assumed based on filename)

With INFO logging on the UAG we weren't able to determine if a malicious payload had been sent. In the ESMANAGER log successful connections were not logged.

We could see the connection on the backend connection server however we could not determine this was a malicious payload in the default logging configuration.

in DEBUG mode we could see the connections and PALOADS on the UAG.

### Exploitation Entry Points

There are at least two pages on the HTML Access services that are vulnerable when ther server are unpatched:

- /broker/xml
- /portal/info.jsp

*Please note we've had mixed results with /brokes/xml which may be build version specific.*

## Threat Intel

Micosoft has reported DEV-0401 using Log4Shell in relation to ransomware activity:

"We have observed a China-based ransomware operator that we're tracking as DEV-0401 exploiting the CVE-2021-44228 vulnerability in Log4j 2 (aka **#log4shell**) targeting internet-facing systems running VMWare Horizon. <https://t.co/6GOdRwRTjk>

— Microsoft Security Intelligence (@MsftSecIntel) **January 11, 2022**

## Advisory

This post will likely be updated, it's not a step by step of how to find all the evil but it hopefully will help identify malcious activity seen in the real world. We will update this if new intel comes in.

Also if you want to write nicer detections feel free 😊 these are just examples and are by no means the only ways to do this!

# Exploitation Tutorial

When people have had more time to patch and the landscape looks better we will blog how to exploit this and talk about why the currently known backdoor has some limitations due to the service architecture and how the backdoor has been created. It's important to share exploitation knowledge but there are things to consider, if you are sharing exploitation without detection rules / tools this creates a risk to people. VMware products and services are leveraged by organisations worldwide and the log4j RCE on horizon let alone the backdoor can be leveraged for high impact actions by threat actors.

# Thanks

Thanks to everyone in the community and industry who has and is helping, thanks to all of those who have stayed up late, missed family events and generally been super helpful either indirectly or directly. There are lots of people involved in this world who everyday work to keep people safe! (also to my friends and family who have put up with my not being round much!).

◀ **Post Business Email Compromise actions for Office 365 Users**  
**The difference between what can be vs what often is – Cyber Architecture** ▶

---

🔗 blue team connection server CVE-2021-44228 cyber cybercrime CyberSecurity education firewall guides horizon load balancer log4j log4shell logging management Risk Security SIEM uag VMware

---

# Related articles



| Hunting for common Active Directory...



| Threat Analysis Tools



| Cisco IOS XE Incident Upc

Copyright (c) Xservus Limited

