THREAT BULLETINS

Health-ISAC Member Observes Exploitation of Log4Shell Vulnerabilities Targeting VMware Horizon Clients for Malicious Web Shells

TLP:WHITE

Jan 05, 2022

Health-ISAC Threat Operations Center (TOC) has received a new intelligence report from the National Health Service (NHS) regarding an unknown threat group weaponizing Log4Shell to target VMware Horizon Clients in order to install malicious web shells. Health-ISAC has released separate, initial alerts regarding Log4j, which can be accessed here and here. The NHS report's contents can be found in this alert below:

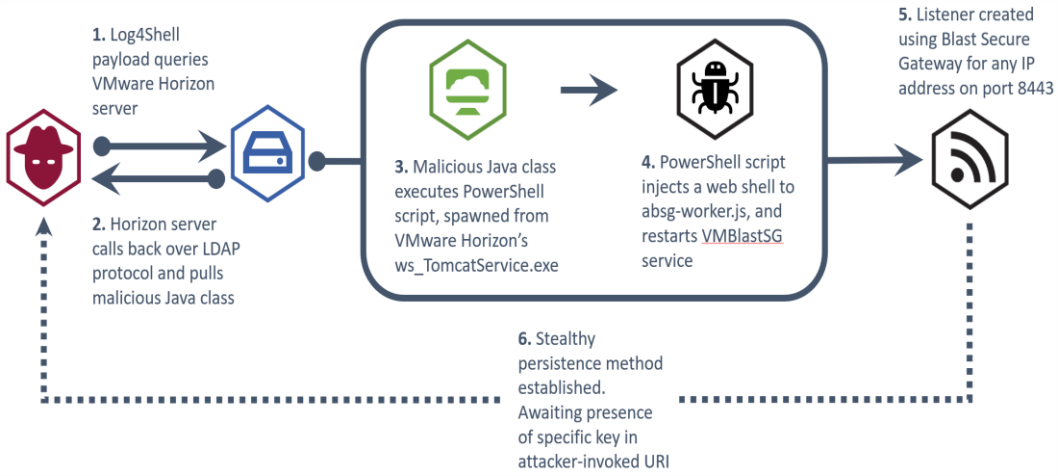
An unknown threat group has been observed targeting VMware Horizon servers running versions affected by Log4Shell vulnerabilities in order to establish persistence within affected networks. According to NHS, the attack likely consists of a reconnaissance phase, where the attacker uses

the Java Naming and Directory Interface (JNDI) via Log4Shell payloads to call back to malicious infrastructure.

Once a weakness has been identified, the attack then uses the Lightweight Directory Access Protocol (LDAP) to retrieve and execute a malicious Java class file that injects a web shell into the VM Blast Secure Gateway service. The web shell can then be used by an attacker to carry out a number of malicious activities such as deploying additional malicious software, data exfiltration, or deployment of ransomware.

The full, original NHS report can be accessed here.

A representative diagram of the attack, provided by NHS, can be accessed below:



Reference(s)	Health-ISAC, Digital, Health-ISAC, amazonaws, Gov.UK

Recommendations
Organizations should look for the following:

- Evidence of *ws_TomcatService.exe* spawning abnormal processes

- Any *powershell.exe* processes containing ‘VMBlastSG’ in the command line
- File modifications to ‘…\VMware\VMware View\Server\appblastgateway\lib\absg-worker.js’
    - This file is generally overwritten during upgrades, and not modified

The NHS has released a PowerShell command to detect VMWare file modification:

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

The NHS has also released a Microsoft Defender for Endpoint query to detect abnormal child processes spawned by ws_TomcatService.exe:

```
1|DeviceProcessEvents
2||where InitiatingProcessFileName =~ "ws_TomcatService.exe"
3|| where FileName != "repadmin.exe"
```

The NHS has also released a Microsoft Defender for Endpoint query to detect powershell.exe processes with 'VMBlastSG' in the command line:

```
1|DeviceProcessEvents
2||where FileName =~ "powershell.exe"
3|| where ProcessCommandLine has "VMBlastSG"
```

Affected organizations should review the VMware Horizon section of the VMware security advisory VMSA-2021-0028 and apply the relevant updates or mitigations immediately.

Sources
NHS: Log4Shell Vulnerabilities in VMware Horizon Targeted to Install Web Shells

Health-ISAC: Update: CISA Releases Open-Source Log4j Vulnerability Scanner

Health-ISAC: Update: CISA Releases Central Guide and Affected Product Repository for Log4j Vulnerability

Alert ID 9abfd78c

View Alert

Tags log4shell, Log4j, VMWare Horizon Client, VMware Horizon, VMware

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App. 

For more update and alerts, visit: **https://health-isac.cyware.com**