Miles de servidores Vmware ESXi atacados con ransomware mediante vulnerabilidades críticas

El viernes y durante el fin de semana, varios equipos de respuesta a emergencias informáticas (CERT) hicieron sonar la alarma sobre un ataque de ransomware a gran escala en curso en máquinas virtuales VMware ESXi.

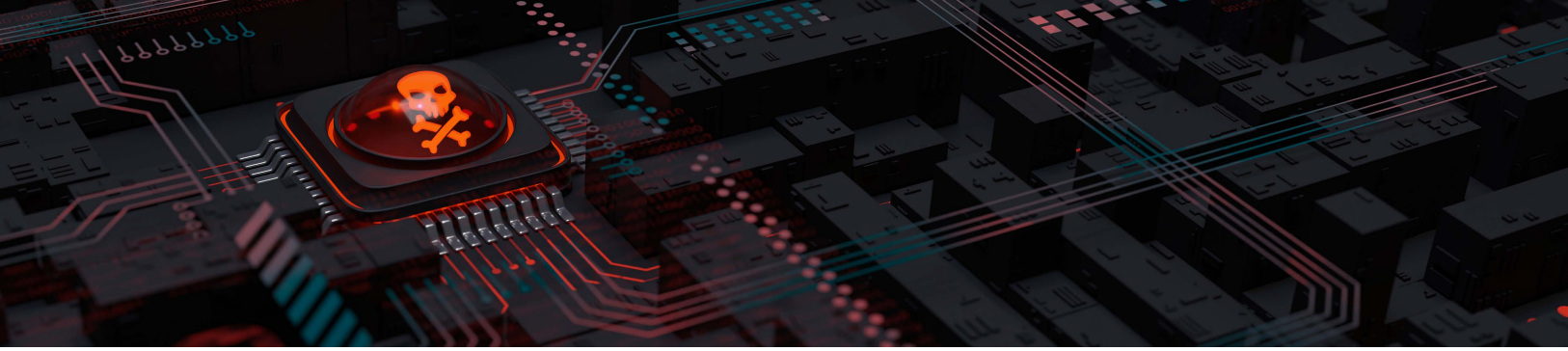
Con algunas discrepancias entre las consultas de Shodan de varios investigadores, la mayoría está de acuerdo en que aproximadamente 500 entidades se vieron afectadas por el ataque durante el fin de semana.

Vulnerabilidad antigua

La vulnerabilidad sospechosa, que aparece como **CVE-2021-21974,** fue parcheada por VMware hace casi dos años. La vulnerabilidad se puede encontrar en OpenSLP tal como se usa en **ESXi** (7.0 antes de ESXi70U1c-17325551, 6.7 antes de ESXi670-202102401-SG, 6.5 antes de ESXi650-202102101-SG) y es una vulnerabilidad de desbordamiento de montón. Un actor malintencionado que reside en el mismo segmento de red que ESXi que tiene acceso al puerto 427 puede desencadenar el problema de desbordamiento del montón en el servicio OpenSLP, lo que resulta en la ejecución remota de código.

Un desbordamiento de búfer es un tipo de **vulnerabilidad de software** que existe cuando un área de memoria dentro de una aplicación de software alcanza su límite de dirección y escribe en una región de memoria adyacente.

En el código de explotación de software, dos áreas comunes que están destinadas a los desbordamientos son la pila y el montón. La memoria de montón es utilizada por todas las partes de una aplicación en lugar de la memoria de pila que es utilizada por un solo subproceso de ejecución.



Mitigación

Los productos vulnerables para CVE-2021-21974 son VMware ESXi y VMware Cloud Foundation (Cloud Foundation). Para corregir CVE-2021-21974, aplique las actualizaciones enumeradas en 3b en la columna "Versión corregida" de la "Matriz de respuesta" a las implementaciones afectadas.
Las versiones fijas son:

- Para ESXi 7.0: ESXi70U1c-17325551 o posterior
- Para ESXi 6.7: ESXi670-202102401-SG o posterior
- Para ESXi 6.5: ESXi650-202102101-SG o posterior
- Para Cloud Foundation (ESXi) 4.x: 4.2 o posterior
- Para Cloud Foundation (ESXi) 3.x: consulte el artículo KB82705 KbMtes de VMware
  Una solución alternativa recomendada si no usa el servicio OpenSLP en ESXi es deshabilitar el servicio SLP en VMware ESXi.

Ransomware

A pesar de que las instrucciones de prueba de concepto (PoC) se publicaron solo unos meses después de que se parcheó la vulnerabilidad, no hemos visto ningún informe de que el exploit se haya utilizado en la naturaleza antes del 3 de febrero de 2023. El ataque estaba dirigido a servidores ESXi vulnerables que están expuestos a Internet en el puerto 427. El actor de amenazas ejecuta un proceso de cifrado dirigido específicamente a archivos de máquinas virtuales (".vmdk", ".vmx", ".vmxf", ".vmsd", ".vmsn", ".vswp", ".vmss", ".nvram","*.vmem"). Aunque algunos investigadores han encontrado casos en los que solo se cifraron los archivos de configuración. Más sobre eso más adelante.

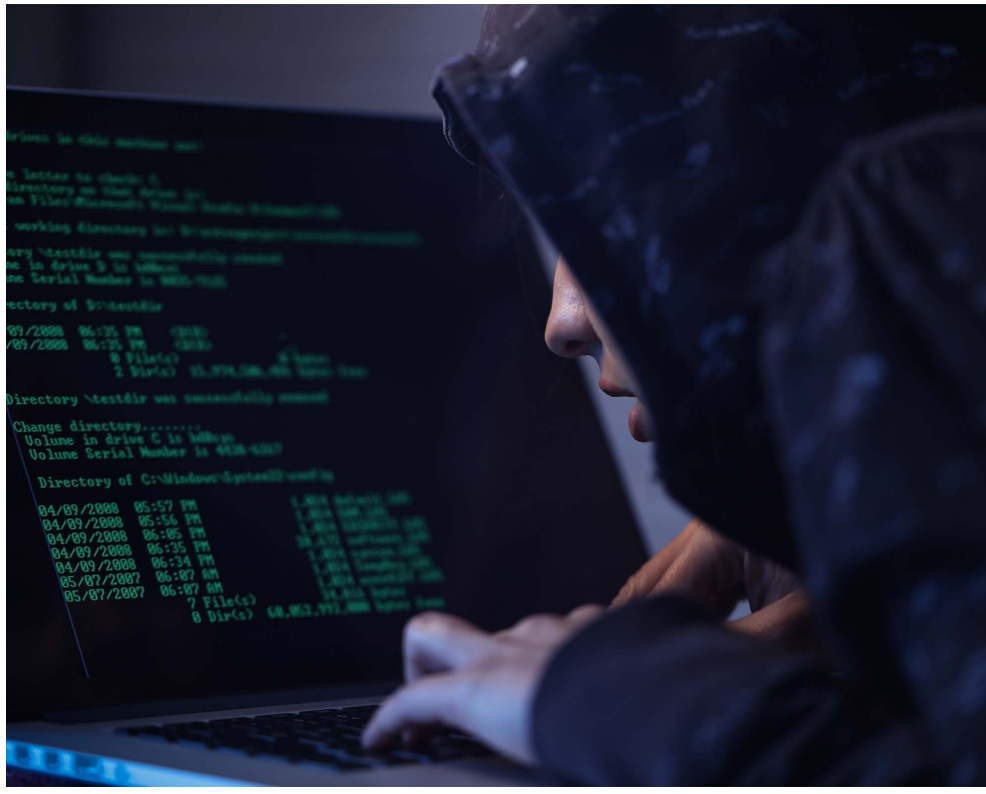
Se cree que el grupo de ransomware que supuestamente lanzó este ataque a gran escala denominado ESXiArgs contra ESXi vulnerable es el nuevo grupo de ransomware de Nevada.

Recientemente, se supo que el grupo de ransomware Royal había agregado la capacidad de **apuntar a máquinas Linux a su arsenal.** Con la transición de las organizaciones a máquinas virtuales (VM), una versión de ransomware basada en Linux les permite dirigirse a las máquinas virtuales ESXi muy populares.

Descifrable

El investigador de seguridad Matthieu Garin publicó en las redes sociales que **los atacantes solo cifran los archivos de configuración,** y no los discos vmdk donde se almacenan los datos. En tales casos, el sitio web **Enes.dev** puede ser de ayuda para usted. La guía explica cómo los administradores pueden reconstruir sus máquinas virtuales y recuperar sus datos de forma gratuita.

Según una investigación de BleepingComputer, la rutina de cifrado en sí es segura, lo que significa que no hay errores de criptografía que permitan el descifrado gratuito.



Renuncias

Nevada puede llegar a ser la variante de Linux de un conocido grupo de ransomware.

Si bien todas las pistas apuntan a **CVE-2021-21974,** existen varias vulnerabilidades críticas en VMware ESXi como CVE-2022-31696, CVE-2022-31697, CVE-2022-31698 y CVE-2022-31699, que pueden conducir potencialmente a la ejecución remota de código (RCE) en los sistemas afectados.

Puede haber circunstancias especiales en el trabajo en los casos en que solo se cifraron los archivos de configuración. Por ejemplo, el ransomware intenta detener la máquina virtual para que pueda cifrar el archivo, pero esto no siempre puede tener éxito en cuyo caso el daño se limita a los archivos de configuración.

Fuente de información:
malwarebytes.com