VMware abordó varias vulnerabilidades críticas de ejecución remota de código (RCE) en la plataforma de administración de infraestructura virtual VMware ESXi y vSphere Client, que pueden permitir a los atacantes ejecutar comandos arbitrarios y tomar el control de los sistemas afectados.

> *«Un agente malicioso con acceso a la red al puerto 445 puede aprovechar este problema para ejecutar comandos con privilegios sin restricciones en el sistema operativo subyacente con anfitriones vCenter Server»,* dijo la compañía.

La vulnerabilidad, rastreada como CVE-2021-21972, con puntuación CVSS de 9.8, es crítica en gravedad.

> *«En nuestra opinión, la vulnerabilidad RCE en vCenter Server no puede representar una amenaza menor que la infame vulnerabilidad en Citrix (CVE-2019-19781)»,* dijo Mikhail Klyuchnikov, de Positive Technologies.
>
> *«El error permite que un usuario no autorizado envíe una solicitud especialmente diseñada, que luego les dará la oportunidad de ejecutar comandos arbitrarios en el servidor».*

Con este acceso en su lugar, el atacante puede moverse con éxito a través de la red corporativa y obtener acceso a los datos almacenados en el sistema vulnerable, como información sobre máquinas virtuales y usuarios del sistema, dijo Klyuchnikov.

Por otro lado, una segunda vulnerabilidad, rastreada como CVE-2021-21973 y con puntuación CVSS de 5.3, permite a los usuarios no autorizados enviar solicitudes POST, lo que puede permitir a un atacante realizar más ataques, incluyendo la capacidad de escanear la red interna de la compañía y recuperar información específica sobre los puertos abiertos de

varios servicios.

El problema de divulgación de la información, según VMware, se debe a una vulnerabilidad SSRF (Server Side Request Forgery) debido a una validación incorrecta de las URL en el complemento vCenter Server.

VMware también proporcionó soluciones para corregir temporalmente CVE-2021-21972 y CVE-2021-21973 hasta que se puedan implementar las actualizaciones. Los pasos detallados se encuentran aquí.

Cabe mencionar que VMware solucionó una vulnerabilidad de inyección de comandos en su producto vSphere Replication (CVE-2021-21976) a inicios de febrero, que podría otorgar a un atacante privilegios administrativos para ejecutar comandos de shell y realizar RCE.

Finalmente, VMware resolvió un error de desbordamiento de pila (CVE-2021-21974) en el protocolo de ubicación del servicio (SLP) de ESXi, lo que potencialmente permite que un atacante en la misma red envíe solicitudes SLP maliciosas a un dispositivo ESXi y tome el control de ella.

OpenSLP proporciona un marco para permitir que las aplicaciones de red descubran la existencia, ubicación y configuración de servicios en red en redes empresariales.

La última solución para ESXi OpenSLP viene inmediatamente después de un parche parecido (CVE-2020-3992) en noviembre pasado que podría aprovecharse para activar un uso después de la liberación en el servicio OpenSLP, lo que lleva finalmente a la ejecución remota de código.

Después, surgieron informes de intentos de explotación activos en la naturaleza, con bandas de ransomware que abusaron de la vulnerabilidad para hacerse cargo de máquinas virtuales sin parches implementadas en entornos empresariales y cifrar sus discos duros virtuales.

Se recomienda a los usuarios que instalen las actualizaciones para reducir el riesgo asociado

con las vulnerabilidades, además de *«eliminar las interfaces de vCenter Server del perímetro de las organizaciones, si están allí, y asignarlas a una VLAN separada con una lista de acceso limitado en la red interna».*