Los hipervisores VMware ESXi están siendo objetivo de una nueva ola de ataques diseñados para implementar ransomware en sistemas comprometidos.

> *«Estas campañas de ataque parecen explotar CVE-2021-21974, para la cual, existe un parche disponible desde el 23 de febrero de 2021″*, dijo el Equipo de Respuesta a Emergencias Informáticas (CERT) de Francia.

VMware, en su propia alerta publicada en ese momento, describió el problema como una vulnerabilidad de desbordamiento de pila de OpenSLP, que podría conducir a la ejecución de código arbitrario.

> *«Un actor malintencionado que resida en el mismo segmento de red que ESXi y que tenga 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»*, dijo VMware.

El proveedor francés de servicios en la nube OVHcloud, dijo que los ataques se están detectando a nivel mundial con un enfoque específico en Europa. Se sospecha que las intrusiones están relacionadas con una nueva cepa de ransomware basada en Rust llamada Nevada, que apareció en diciembre de 2022.

Otras familias de ransomware que se sabe que han adoptado Rust en los últimos meses incluyen BlackCat, Hive, Luna, Nokoyawa, RansomExx y Agenda.

> *«Los actores están invitando a los afiliados de habla rusa e inglesa a colaborar con una gran cantidad de agentes de acceso inicial (IAB) en la web oscura»*, dijo Resecurity el mes pasado.

> *«Particularmente, el grupo detrás de Nevada Ransomware también está comprando acceso comprometido por sí mismo, el grupo tiene un equipo dedicado para la explotación posterior y para realizar intrusiones en la red de los objetivos de interés».*

Sin embargo, Bleeping Computer informa que las notas de rescate vistas en los ataques no tienen similitudes con el ransomware de Nevada, y agrega que la tensión se rastrea con el nombre de ESXiArgs.

Se recomienda a los usuarios que actualicen a la última versión de ESXi para mitigar posibles amenazas y restringir el acceso al servicio OpenSLP a direcciones IP de confianza.