Se descubrió que el grupo patrocinado por el estado chino conocido como UNC3886, está explotando una vulnerabilidad de día cero en los hosts VMware ESXi para sistemas Windows y Linux de puerta trasera.

La vulnerabilidad de omisión de autenticación de VMware Tools, rastreada como CVE-2023-20867 (puntaje CVSS: 3.9), *«permitió la ejecución de comandos privilegiados en máquinas virtuales invitadas de Windows, Linux y PhotonOS (cVenter) sin autenticación de credenciales de initado de un host ESXi comprometido y sin inicio de sesión predeterminado en las máquinas virtuales invitadas»,* dijo Mandiant.

UNC3886 fue documentado por primera vez por la compañía de seguridad propiedad de Google, en septiembre de 2002 como un actor de espionaje cibernético que infectaba los servidores VMWare ESXi y vCenter con backdoors denominadas VIRTUALPITA y VIRTUALPIE.

A inicios de marzo, el grupo estuvo vinculado a la explotación de una vulnerabilidad de seguridad de gravedad media, ya parcheada, en el sistema operativo Fortinet FortiOS para implementar planes en los dispositivos de red e interactuar con el malware antes mencionado.

El atacante ha sido descrito como un colectivo adversario *«altamente experto»* que se enfoca en organizaciones de defensa, tecnología y telecomunicaciones en Estados Unidos, Japón y la región de Asia-Pacífico.

«El grupo tiene acceso a una amplia investigación y apoyo para comprender la tecnología subyacente de los dispositivos a los que se dirige», dijeron loa investigadores de Mandiant, destacando su patrón de armar fallas en firewall y el software de virtualización que no son compatibles con las soluciones EDR.

Como parte de sus esfuerzos para explotar los sistemas ESXi, también se ha observado que el atacante recopila credenciales de los servidores vCenter y abusa de CVE-2023-20867 para ejecutar comandos y transferir archivos hacia y desde máquinas virtuales invitadas desde un host ESXi comprometido.

Un aspecto notable del oficio de UNC3886 es su uso de sockets de interfaz de comunicación de máquina virtual (VMCI) para el movimiento lateral y la persistencia continua, lo que le permite establecer un canal encubierto entre el host ESXi y sus máquinas virtuales invitadas.

> *«Este canal de comunicación abierto entre el invitado y el host, donde cualquiera de los roles puede actuar como cliente o servidor, ha permitido un nuevo medio de persistencia para recuperar el acceso en un host ESXi con puerta trasera siempre que se implemente una backdoor y el atacante obtenga acceso inicial a cualquier máquina invitada»,* dijo la compañía.

El desarrollo se produce cuando la investigadora de Summoning Team, Sina Kheirkhah, reveló tres vulnerabilidades distintas en VMware Aria Operations for Networks (CVE-2023-20867, CVE-2023-20888 y CVE-202320889) que podrían resultar en la ejecución remota de código.

> *«UNC3886 sigue presentando desafíos para los investigadores al deshabilitar y manipular los servicios de registro, eliminando selectivamente los eventos de registro relacionados con su actividad. La limpieza retroactiva de los actores de amenazas realizada a los pocos días de las revelaciones públicas anteriores sobre su actividad indican cuán alertas están»,* dijo.