ALERTA DE SEGURIDAD DIGITAL

COLCERT AL-2304-024

EXPLOTACIÓN ZERO-DAY EN VMWARE ESXI SHELL

Se ha reportado un exploit Zero-Day altamente crítico que afecta a VMware ESXi versiones 7.x y 8.x. Este permite la carga remota no autenticada y ejecución de comandos en el servidor ESXi, poniendo en riesgo la integridad y confidencialidad de todas las máquinas virtuales gestionadas por estos servidores.

Riesgo Potencial:

La vulnerabilidad permite el acceso y control no autorizados sobre las máquinas virtuales alojadas en servidores VMware ESXi, lo que podría resultar en una violación masiva de datos internos y de clientes. Además, podría provocar importantes tiempos de inactividad y pérdidas financieras al afectar sistemas operativos críticos.

Detalles técnicos

- **Vulnerabilidad:** Ejecución remota de código vía ESXi Shell.
- **Impacto:** Compromiso total del sistema VMware ESXi y todas las máquinas virtuales alojadas.
- **Método de Explotación:** Omitir autenticación en el servicio ESXi Shell para cargar archivos maliciosos.
- **Requisitos para Explotación:** ESXi Shell activado, IPv4 configurado como primario, sistema corriendo vSphereESXi 7.x/8.x.

Recomendaciones:

- Verificar la versión actual del sistema VMware ESXi para determinar si es vulnerable.
- Aplicar parches proporcionados por VMware inmediatamente para cerrar la brecha de seguridad.
- Realizar monitoreo continuo de la actividad de red para detectar comportamientos inusuales.
- Realizar auditorías de seguridad y comprobaciones de cumplimiento periódicamente para abordar vulnerabilidades.

Acción sugerida

Para enfrentar las amenazas actuales de seguridad, es imperativo que todas las organizaciones que operan sistemas VMware ESXi actúen con celeridad aplicando los parches correspondientes. Esto garantizará la protección ante las vulnerabilidades severas recientemente identificadas.
Consulte las instrucciones detalladas de mitigación disponibles en la página oficial de VMware a través del siguiente enlace: Mitigación de vulnerabilidades para VMware ESXi. (https://kb.vmware.com/s/article/88632)

Precio de Explotación: El Exploit se ofrece en el mercado negro por un precio de $1,500,000 pagables en Monero, lo que indica un alto valor percibido por los atacantes debido a su potencial destructivo.

FUENTES:

1.https://blog.segu-info.com.ar/2024/04/exploit-zero-day-contra-vmware-esxi.html
2.https://unaaldia.hispasec.com/2023/06/ciberdelincuentes-chinos-explotan-vulnerabilidad-zero-day-de-vmware-en-sistemas-windows-y-linux.html
3.https://www.ciberseguridadlatam.com/2024/03/10/vmware-corrige-errores-criticos-e-importantes-en-esxi-workstation-y-fusion/
4.http://www3.cvh.edu.mx/comunidad-cvh/

COLCERT