Vulnerabilidades en VSA de KASEYA

El Equipo de Respuesta de Incidentes de Seguridad de la Información EcuCERT, alerta sobre un ramsomware que afecta al software VSA de Kaseya.

En conocimiento del reporte realizado desde nuestras redes de confianza internacionales ante el reciente ataque de ransomware de la cadena de suministro aprovechando una vulnerabilidad en el software VSA Kaseya contra múltiples proveedores de servicios administrados (MSP) y sus clientes.

Un Proveedor de Servicios Administrados (MSP) es una empresa que administra de forma remota la infraestructura de IT de un cliente y/o sistemas de usuario final, normalmente de forma proactiva y bajo un modelo de suscripción.

El EcuCERT insta a los MSP afectados y a sus clientes a que sigan los siguientes pasos:

A los MSP:

1. Descargue la herramienta de detección Kaseya VSA . Esta herramienta analiza un sistema (ya sea servidor VSA o punto final administrado) y determina si hay algún indicador de compromiso (IOC) presente.
2. Habilite y aplique la autenticación multifactor (MFA) en cada cuenta que esté bajo el control de la organización y, en la mayor medida posible, habilite y aplique MFA para los servicios de cara al cliente.
3. Implementar listas de permisos para limitar la comunicación con capacidades de administración y monitoreo remoto (RMM) a pares de direcciones IP conocidos, y / o
4. Coloque las interfaces administrativas de RMM detrás de una red privada virtual (VPN) o un firewall en una red administrativa dedicada.

Se recomienda a los clientes de MSP afectados por este ataque que tomen medidas inmediatas para implementar las siguientes mejores prácticas de ciberseguridad. **Nota:** estas acciones son especialmente importantes para los

clientes de MSP que actualmente no tienen su servicio RMM en ejecución debido al ataque de Kaseya.

1. Asegúrese de que las copias de seguridad estén actualizadas y almacenadas en una ubicación fácilmente recuperable que esté separada de la red de la organización;
2. Revertir a un proceso de administración de parches manual que sigue las pautas de corrección del proveedor, incluida la instalación de nuevos parches tan pronto como estén disponibles;

Implementar:

1. Autenticación multifactor; y
2. Principio de privilegio mínimo en cuentas de administrador de recursos de red clave.

Recursos:

Nuestros proveedores de información proporcionan estos recursos:

- Para obtener la orientación más reciente de Kaseya, consulte el Aviso importante de Kaseya del 3 de julio de 2021 .
- Para conocer los indicadores de compromiso, consulte la página REvil Kaseya CnC Domains de Peter Lowe en GitHub .

Referencias:

- Administrador, (04 de julio de 2021). Recuperado 06 de julio de 2021. Obtenido de https://us-cert.cisa.gov/ncas/current-activity/2021/07/04/cisa-fbi-guidance-msps-and-their-customers-affected-kaseya-vsa