INFORME: 10CND22-00084-02
TLP: BLANCO

ALERTA DE SEGURIDAD CIBERNÉTICA
ACTUALIZACIÓN SOBRE VULNERABILIDAD DÍA 0 EN MICROSOFT EXCHANGE

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT de Gobierno, comparte una recomendación entregada por Microsoft sobre dos vulnerabilidades de día cero (CVE-2022-41040, que falsifica solicitudes del lado del servidor; y CVE-2022-41082, permite la ejecución remota de código (RCE) cuando el atacante logra acceder a PowerShell), las cuales afectan a los servidores Exchange en sus versiones 2013, 2016 y 2019.

Mientras se continúa trabajando en un parche para controlar este incidente, Microsoft **recomienda enfáticamente a los clientes de Exchange Server que deshabiliten el acceso remoto a PowerShell para usuarios que no sean administradores en su organización**.

El CSIRT de Gobierno insta a las entidades a seguir las recomendaciones del fabricante, las que están disponibles en el siguiente enlace:
https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/

Adicionalmente, se reitera la solicitud realizada en la alerta emitida el pasado viernes 30 de septiembre, para que las organizaciones de la Administración Pública, las entidades en convenio de colaboración y las entidades privadas y el público en general, evalúen la posibilidad de suspender la disponibilidad de Exchange desde cualquier geolocalización fuera de Chile mientras no exista un parche definitivo para estas vulnerabilidad, solo como medida extrema y entendiendo el contexto específico de explotación de las vulnerabilidades de los servidores Exchange en nuestro país conocido en las recientes semanas.

Complementariamente, solicitamos a las organizaciones para que realicen un análisis de registro a nivel de servidor y servicios para descartar o verificar la existencia de compromiso de sus sistemas y reiteramos la la importancia de instalar antivirus a nivel de servidor.

CSIRT
Gobierno
de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.10.03 12:27:31 -03'00'