INFORME: 10CND22-00084-04
TLP: BLANCO

ALERTA DE SEGURIDAD CIBERNÉTICA
RECIENTE ACTUALIZACIÓN SOBRE VULNERABILIDAD DÍA CERO EN MICROSOFT EXCHANGE

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT de Gobierno, comparte una nueva actualización de las recomendaciones entregadas por Microsoft este miércoles 5 de octubre sobre las vulnerabilidades de día cero descubiertas la semana pasada (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.

Esta jornada, Microsoft informó a sus clientes de Exchange Server que las mitigaciones recomendadas en su blog deben completarse para ambos parches.

El informe del fabricante señala explícitamente que "*los clientes de Exchange Server deben completar la mitigación de la regla de reescritura de URL para CVE-2022-41040 y la mitigación de deshabilitar PowerShell remoto para no administradores para CVE-2022-41082 que se describe a continuación*".

El detalle de la actualización está disponible en el blog de la empresa para esta vulnerabilidad en el enlace: https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/

El CSIRT de Gobierno llama a las organizaciones a permanecer alertas a nuevas actualizaciones mientras el fabricante continúa trabajando en un parche para dar una solución definitiva del problema.

De la misma manera, insistimos en la recomendación para que las organizaciones 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 importancia de instalar antivirus a nivel de servidor.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.10.05 23:48:05 -03'00'