INFORME: 10CND22-00084-03
TLP: BLANCO

ALERTA DE SEGURIDAD CIBERNÉTICA
NUEVA 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 recomendación entregada por Microsoft este 4 de octubre 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 Microsoft continúa trabajando en un parche para controlar este incidente, el fabricante recomienda a sus clientes revisar la sección de mitigaciones de su blog las que mejoran las reglas de escritura de URL.

Las recomendaciones específicas que entrega Microsoft apuntan a las siguientes opciones:

- "Opción 1: la regla EEMS se ha actualizado y se está implementando. Se aplicará automáticamente."

  La regla de EEMS (Exchange Emergency Mitigation Service) se ha actualizado y se está implementando para aquellas versiones en parches acumulados que cuentan con este servicio desde septiembre de 2021 para las versiones de Exchange de 2019 (CU11) y 2016 (CU22).

  Para comprobar si su servidor está configurado correctamente con EEMS, ejecute el siguiente comando en Exchange PowerShell:

  - Get-OrganizationConfig | select MitigationsEnabled

  El comando debería retornar un valor "true"

- "Opción 2: el script EOMTv2 proporcionado anteriormente se ha actualizado para incluir la mejora de reescritura de URL."

  En otras palabras, se ha dispuesto un script para EOMTv2 (Exchange On-premises Mitigation Tool, versión 2), el que cumple la función de corregir la configuración anterior. El script está disponible en el siguiente enlace: https://microsoft.github.io/CSS-Exchange/Security/EOMTv2/

- "Opción 3: las instrucciones de la regla de reescritura de URL se han actualizado. La cadena en el paso 6 y el paso 9 ha sido revisada. Los pasos 8, 9 y 10 tienen imágenes actualizadas."

  Hace referencia a la actualización del método originalmente propuesto como mitigación, el que se encuentra disponible en el siguiente enlace: https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/

Finalmente, se insta 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 importancia de instalar antivirus a nivel de servidor.

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.10.04 20:33:28 -03'00'