INFORME: 10CND22-00084-05
TLP: BLANCO

ALERTA DE SEGURIDAD CIBERNÉTICA
SOLICITA A LAS ORGANIZACIONES TOMAR CONOCIMIENTO Y APLICAR LAS MITIGACIONES DEL FABRICANTE SOBRE VULNERABILIDADES DÍA 0 EN MICROSOFT EXCHANGE

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT de Gobierno, comparte la más reciente actualización de las recomendaciones que entrega Microsoft sobre dos vulnerabilidades de día cero que afectan a los servidores Exchange en sus versiones 2013, 2016 y 2019, las cuales aún no cuentan con un parche definitivo.

Las vulnerabilidades son:

- CVE-2022-41040, que falsifica solicitudes del lado del servidor;
- y CVE-2022-41082, que permite la ejecución remota de código (RCE) cuando el atacante logra acceder a PowerShell).

En la más reciente entrega de su *Guía para el cliente*, Microsoft indicó que se realizaron actualizaciones en la regla de reescritura de URL, por lo cual solicita a sus clientes revisar y utilizar algunas de las opciones que allí se sugieren.

El fabricante señaló que la mitigación para EEMS se actualizó y se aplicará de manera automática; además indicó que se actualizó la mitigación para EOMTv2; y solicitó a sus clientes revisar los pasos 8, 9 y 10 de la cadena de la regla de escritura, las que cuentan con imágenes nuevas.

El detalle de la actualización está disponible en el blog de la empresa 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 y aplicar las mitigaciones informadas en las actualizaciones entregadas por el fabricante mientras éste continúa trabajando en un parche para dar solución definitiva del problema, dado que **la posibilidad de la explotación de la vulnerabilidad es real**.

De la misma manera, insistimos en las recomendaciones para que las organizaciones evalúen la posibilidad de suspender la disponibilidad de Exchange fuera de Chile mientas no exista un parche definitivo para estas vulnerabilidades, y 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.

Por último, queremos señalar a la comunidad en general, que la intrusión en organizaciones explotando las vulnerabilidades de un sistema informático sin la autorización expresa de ésta, aun cuando su finalidad sea con fines científicos, está expresamente prohibido por la vigente Ley de Delitos Informáticos en Chile.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.10.08 12:12:47 -03'00'