INFORME: 10CND22-00084-06
TLP: BLANCO

ALERTA DE SEGURIDAD CIBERNÉTICA
MICROSOFT LANZA PARCHES PARA VULNERABILIDADES DÍA 0 EN EXCHANGE

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT de Gobierno, informa que Microsoft finalmente ha publicado parches para 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), conocidas en septiembre y apodadas ProxyNotShell, las cuales afectan a los servidores Exchange en sus versiones 2013, 2016 y 2019.

Es necesario que los encargados de ciberseguridad de las instituciones implementen estas actualizaciones cuanto antes.

La información entregada por Microsoft para la descarga e instalación de los parches se encuentra aquí, aunque también se señala que son parte de la más reciente actualización de Windows Update:
https://support.microsoft.com/en-us/topic/description-of-the-security-update-for-microsoft-exchange-server-2019-2016-and-2013-november-8-2022-kb5019758-2b3b039b-68b9-4f35-9064-6b286f495b1d

El CSIRT de Gobierno compartió, durante octubre, noticias y mitigaciones relativas a las vulnerabilidades CVE-2022-41040 y CVE-2022-41082, documentos que pueden ser revisados en:
https://www.csirt.gob.cl/noticias/10cnd22-00084-01/
https://www.csirt.gob.cl/noticias/10cnd22-00084-02/
https://www.csirt.gob.cl/noticias/10cnd22-00084-03/
https://www.csirt.gob.cl/noticias/10cnd22-00084-04/
https://www.csirt.gob.cl/noticias/10cnd22-00084-05/

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.11.08 22:11:53 -03'00'