TLP: BLANCO

ALERTA DE SEGURIDAD CIBERNÉTICA
SE REITERA NECESIDAD DE PARCHAR VULNERABILIDADES CRÍTICAS EN SERVIDORES DE CORREO

El CSIRT de Gobierno quiere hacer un llamado a las instituciones públicas del Estado, a las entidades en convenio de colaboración y a los administradores de sistemas y público en general, para que tomen medidas de carácter preventivo para subsanar una vulnerabilidad en el servidor Exchange de Microsoft (CV·-2021-34473), cuyo parche está disponible desde julio de 2021 en el siguiente enlace: https://www.csirt.gob.cl/media/2021/07/9VSA21-00466-01.pdf

El CSIRT de Gobierno ha compartido y advertido, al menos en tres oportunidades anteriores, información con respecto a la criticidad de esta vulnerabilidad, tanto en su publicación original cuando el fabricante llamó a su parchado, así como en otros dos eventos posteriores:

- En marzo de 2022, en el contexto del ataque de ransomware AvosLocker (el que apuntaba contra máquinas virtuales de VMware) https://www.csirt.gob.cl/media/2022/03/10CND22-00059-01-Alerta-AvosLocker-2022-03.pdf

- Y en abril de 2022, siguiendo una recomendación global urgente expresada por la agencia federal estadounidense CISA por la explotación activa de la vulnerabilidad en ese momento. https://www.csirt.gob.cl/noticias/listado-vulnerabilidades-cisa/

De igual manera, CSIRT aprovecha este contexto para sugerir a las instituciones que revisen el estado de la seguridad en los servidores de correos basados en Zimbra vinculados a la vulnerabilidad CVE-2022-37042, siguiendo las indicaciones publicadas el pasado mes de agosto y que están disponibles en el siguiente enlace: https://csirt.gob.cl/noticias/vulnerabilidad-autenticacion-zimbra/

Se recomienda a las organizaciones que utilizan estos servicios (Exchange y Zimbra) revisar si los parches recomendados por el fabricante fueron aplicados y, de no ser así, realizar las gestiones para actualizarlos de manera urgente.

De igual manera, se insta a los administradores para que auditen los logs de sus servidores de correos en busca de patrones maliciosos o sospechosos. De encontrarlos, pueden comunicarse con el CSIRT de Gobierno al correo soc@interior.gob.cl o al teléfono 1510, ambos disponibles en modalidad 24/7.

CSIRT
Gobierno
de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.09.22 16:29:58 -03'00'