ALERTA DE SEGURIDAD DE LA INFORMACIÓN
NUEVAS VULNERABILIDADES DE DÍA CERO
EN MICROSOFT EXCHANGE
TLP: BLANCO

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT de Gobierno) del Ministerio del Interior y Seguridad Pública comparte con la comunidad información relacionada con cuatro vulnerabilidades de día cero identificadas por la Zero Day Initiative y que afectan a Microsoft Exchange.

Las vulnerabilidades aún no cuentan con CVE, siendo identificadas por la Zero Day Initiative según sus propios códigos de seguimiento de vulnerabilidades como:

- ZDI-23-1578: Vulnerabilidad de ejecución remota de código, CVSS: 7,5 (https://www.zerodayinitiative.com/advisories/ZDI-23-1578/).
- ZDI-23-1579: Vulnerabilidad de divulgación de información, CVSS: 7,1 (https://www.zerodayinitiative.com/advisories/ZDI-23-1579/).
- ZDI-23-1580: Vulnerabilidad de divulgación de información, CVSS: 7,1 (https://www.zerodayinitiative.com/advisories/ZDI-23-1580/).
- ZDI-23-1581: Vulnerabilidad de divulgación de información, CVSS: 7,1 (https://www.zerodayinitiative.com/advisories/ZDI-23-1581/).

A la fecha, Microsoft no ha hecho disponibles parches para contrarrestar estas vulnerabilidades. Tampoco existen medidas de mitigación. **En vista de lo anterior, reforzamos la necesidad de mantener una actitud vigilante respecto de cualquier cambio sospechoso que pueda observarse en las cuentas de Exchange de su institución,** siguiendo las recomendaciones que entregamos a continuación:

- Chequear los logs de Microsoft Exchange desde al menos el 15 de octubre.
- Revisar si existen accesos a cuentas de correo efectuados desde fuera de un área geográfica razonable (como puede ser Chile, o las regiones desde donde se conectan normalmente sus trabajadores) y en horarios poco comunes.
- Implementar sistemas de doble factor de autenticación para las cuentas de email.
- Auditar su tráfico de red.
- Forzar un escaneo completo, desactivando la opción de solo analizar archivos nuevos.

Recuerden que ante cualquier consulta, siempre pueden escribir al CSIRT de Gobierno al correo electrónico incidentes@interior.gob.cl, o llamar al 1510.

Más información: Múltiples vulnerabilidades 0day en Microsoft Exchange (Incibe): https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-0day-en-microsoft-exchange

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.11.03 17:11:14 -03'00'