Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA22-00712-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	30 de septiembre de 2022
Última revisión	30 de septiembre de 2022

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del CSIRT de Gobierno. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT de Gobierno, comparte información sobre vulnerabilidades de día cero ("zero day") recientemente conocidas, y que afectan a Microsoft Exchange Server.

Vulnerabilidades

CVE-2022-41040
CVE-2022-41082

Impacto

Vulnerabilidades de riesgo crítico

CVE-2022-41040: Permite la ejecución remota de código (RCE) en los sistemas afectados.
CVE-2022-41082: Permite la ejecución remota de código (RCE) en los sistemas afectados.

Productos afectados

Exchange Server 2013, 2016 y 2019

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor cuando este esté disponible.

Enlaces

https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41040
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41082

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.09.30 09:36:43 -03'00'