Alerta de seguridad cibernética	9VSA21-00400-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	3 de marzo de 2021
Última revisión	3 de marzo de 2021

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 equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información sobre siete vulnerabilidades que afectan a Microsoft Exchange Server.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidades

CVE-2021-26412
CVE-2021-26854
CVE-2021-26855
CVE-2021-26857
CVE-2021-26858
CVE-2021-27065
CVE-2021-27078

Impactos

Cuatro de las vulnerabilidades ya están siendo explotadas activamente, las que son consideradas como de riesgo crítico:

CVE-2021-26857, CVE-2021-26858, CVE-2021-26855 y CVE-2021-27065: Estas vulnerabilidades permiten a un atacante remoto ejecutar código arbitrario en el sistema, debido a una validación insuficiente de la información ingresada por el usuario. Un atacante remoto puede enviar datos especialmente diseñados a un servidor de Exchange y ejecutar código arbitrario en el sistema.

Como de riesgo alto son consideradas:

CVE-2021-26412, CVE-2021-26854 y CVE-2021-27078: Estas vulnerabilidades permiten a un atacante remoto ejecutar código arbitrario en el sistema, debido a una validación insuficiente de la información ingresada por el usuario. Un atacante remoto puede enviar datos especialmente diseñados a un servidor de Exchange y ejecutar código arbitrario en el sistema.

Productos Afectados

Microsoft Exchange Server: Versiones desde la 2013 a la 2019 Cumulative Update 8.

Mitigación

Instalar las últimas actualizaciones de los productos afectados desde el sitio del proveedor.

Enlaces

https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26412

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26854

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26855

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26857

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26858

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27065

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27078

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26412

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26854

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26855

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26857

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26858

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27065

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27078

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.03.11 13:26:22 -03'00'