VULNERABILIDAD EXPLOTA ACTIVAMENTE EN MICROSOFT EXCHANGE (30/AGOSTO/2021)

Vulnerabilidades detectadas en Microsoft Exchange permitirán que ciber atacantes ejecuten programas maliciosos de tipo Ransomware

Microsoft Exchange es una herramienta muy respecto de las aplicaciones disponibles en la categoría ofimática, tales como correo electrónico, calendario, contactos y colaboración en línea. La herramienta se encuentra instalada en el sistema operativo Windows Server de tal manera que todos los usuarios de la red pueden acceder a sus servicios desde cualquier tipo de dispositivo. Las más recientes versiones se encuentran en otros paquetes de software populares tales como Office 365 y opciones de servicio en la nube.

Un fallo detectado en Microsoft Exchange permitiría saltarse los controles definidos en las listas de control de acceso ACL y posteriormente hacer un escalamiento de privilegios del usuario de sesión, lo cual a su vez permite la ejecución remota de cualquier tipo de programa malicioso. El error llamado “ProxyToken” debido al tipo de aplicaciones que tiene acceso, está ligado a varios incidentes de datos personales.

En consideración al alto riesgo contra la confidencialidad, integridad y disponibilidad de los activos de información administrados por la herramienta Microsoft Exchange, el EcuCERT recomienda a su comunidad objetivo, tomar en consideración las siguientes recomendaciones:

1. Aplicar los parches de actualización y mecanismos de contención emitidos por el desarrollador.

2. Ejecutar aplicaciones con perfiles de usuario con el menor privilegio posible.
3. Implementar mecanismos de monitoreo y control de tráfico enfocados en conexiones atípicas.

Referencias

MICROSOFT. 2021. Microsoft Exchange Server Security Feature Bypass Vulnerability. Disponible en https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31207

CVE. 2021. CVE-2021-34523. Disponible en https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34523

CVE. 2021. CVE-2021-31207. Disponible en https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31207

CVE. 2021. CVE-2021-34473. Disponible en https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34473

MICROSOFT. 2021. Released July 2021 Exchange Server Security Updates. Disponible en https://techcommunity.microsoft.com/t5/exchange-team-blog/released-july-2021-exchange-server-security-updates/ba-p/2523421