BOLETÍN DE ALERTA

Boletín Nro.: 2021-31

Fecha de publicación: 25/11/2021

Tema: Vulnerabilidades RCE en Microsoft Exchange.

Versión afectada:

- Microsoft Exchange Server 2016 CU 21 y CU 22.
- Microsoft Exchange Server 2019 CU 10 y CU 11.

Descripción:

La vulnerabilidad identificada como CVE-2021-42321, de severidad alta con una puntuación de 8.8, corresponde a un fallo de ejecución remota de código (RCE) y se debe a una incorrecta validación de los argumentos command-let (cmdlet) que permitiría a un atacante remoto autenticado tomar el control del sistema afectado.

Esta vulnerabilidad es esencialmente un error (bug) en la forma en que Microsoft Exchange permite que se almacenen ciertos datos en la sección "*BinaryData*" de la configuración del usuario; específicamente cuando se establece la configuración del usuario con un "*payload*" en la sección "*BinaryData*" y luego el atacante solicita un token de acceso "*ClientAccessToken*", desencadena un error (bug) que da como resultado la ejecución de dicho "payload".

La vulnerabilidad afecta a Microsoft Exchange Server local, incluidos los servidores utilizados en el modo híbrido.

Debido a la publicación del PoC, se ha registrado un aumento en los intentos de los atacantes de buscar e intentar explotar esta vulnerabilidad, por lo que se recomienda aplicar inmediatamente los parches disponibles.

Impacto:

La explotación exitosa de esta vulnerabilidad podría resultar en que un atacante obtenga privilegios de administración total del componente afectado. Por lo tanto, el atacante podría

instalar programas; ver, cambiar o eliminar datos; o crear nuevas cuentas con todos los privilegios del usuario.

Detección:

El equipo de Microsoft hay proveído de un HealtChecker para verificar si el Servidor Exchange se encuentra vulnerable y el estado del mismo:

- https://microsoft.github.io/CSS-Exchange/Diagnostics/HealthChecker/

Solución:

Verifique que su servidor Microsoft Exchange se encuentre actualizado, específicamente verifique que cuente con los siguientes parches correctamente instalados y aplicados:

- KB5007409 (Noviembre 2021)

Información adicional:

- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-42321
- https://nvd.nist.gov/vuln/detail/CVE-2021-42321