BOLETÍN DE ALERTA

Boletín Nro.: 2021-19

Fecha de publicación: 18/08/2021

Tema: Vulnerabilidades RCE en Microsoft Exchange (ProxyShell).

Fecha de actualización: 19/08/2021

Productos afectados:

- Microsoft Exchange Server 2019.
- Microsoft Exchange Server 2016.
- Microsoft Exchange Server 2013.

Descripción:

ProxyShell es un conjunto de tres fallas de seguridad (CVE-2021-34473, CVE-2021-34523 y CVE-2021-31207) que afectan a Microsoft Exchange Server y que conjuntamente pueden ser explotadas para para lograr ejecutar código arbitrario remotamente sin autenticación. A continuación el detalle de cada una:

1. **CVE-2021-34473 Server Side Request Forgery en Microsoft Exchange Server Autodiscover**

   La falla se encuentra en el servicio de autodescubrimiento (Autodiscover), debido a una validación deficiente de la URI antes de acceder al recurso, omitiendo de esta manera el ACL (Access Control List) y saltando el mecanismo de autenticación.

   Fue parcheada en conjunto a otras vulnerabilidades en abril en KB5001779.

2. **CVE-2021-31207 Escritura arbitraria de archivos RCE en Microsoft Exchange Server**

   Se trata de una falla en el manejo de la exportación de buzones de correo. Debido a una validación deficiente de los datos enviados por el usuario, se puede subir archivos arbitrarios. Esto permite a un atacante remoto autenticado ejecutar código arbitrario en el servidor, en el contexto SYSTEM (privilegiado). Esta falla fue parcheada en mayo por Microsoft en KB5003435.

3. **CVE-2021-34523 Autenticación inadecuada en Microsoft Exchange Server PowerShell**

   Se trata de una falla dentro del servicio Powershell, debido a la falta de una validación adecuada de un token de acceso antes de ejecutar el comando Exchange PowerShell, permitiendo escalar de privilegios.

   La vulnerabilidad de elevación de privilegios fue parcheada por Microsoft en abril en KB5001779.

Estas tres vulnerabilidades pueden ser utilizadas en conjunto por parte de un atacante remoto no autenticado para saltar los mecanismos de autenticación y lograr ejecutar código arbitrario en el contexto de SYSTEM (máximo privilegio), logrando el control total del servidor.

Los detalles técnicos de estas vulnerabilidades, que habían sido descubiertas en el concurso Pwn2Own2021 en abril, fueron presentados en la conferencia Black Hat 2021. Investigadores han detectado que adversarios están actualmente escaneando Internet en busca de servidores afectados por estas tres vulnerabilidades.

Las correcciones de CVE-2021-34473 y CVE-2021-34523 ya habían sido incluidas en el parche de abril y CVE-2021-31207 en el de mayo, sin embargo, existen todavía numerosos servidores que no han sido actualizados, lo cual, sumado a la reciente presentación de los exploits, aumenta el riesgo de ataque a estos servidores vulnerables.

Impacto:

La explotación exitosa de las vulnerabilidades podría permitir a los atacantes remotos el control total del sistema.

Detección:

Atendiendo que se trata de una vulnerabilidad que está siendo escaneada y explotada activamente en Internet, es importante que los administradores, especialmente de servidores vulnerables que están o han estado expuestos luego de la publicación de estas vulnerabilidades, analicen si su servidor ya ha sido explotado o si ha habido intentos de explotación.

Detección de escaneos:

Para detectar un escaneo activo en busca de estas vulnerabilidades, puede consultar los registros de proxy inverso para obtener indicadores de actividad de escaneo:

- Solicitudes web entrantes a través del puerto 443 al **uri_path /autodiscover/autodiscover.json** que contiene una de las siguientes cadenas **("powershell", "mapi/nspi", "mapi/emsmdb", "/EWS", "X-Rps- CAT")** con el código de estado resultante 400, 401 y 404.
- Reglas de YARA para buscar ProxyShell, proporcionadas por el investigador Florian Roth: https://github.com/Neo23x0/signature-base/blob/master/yara/expl_proxyshell.yar

Detección de explotación:

La explotación exitosa de ProxyShell se puede detectar a través de registros de proxy inverso, identificando las solicitudes web entrantes a través del puerto 443 al **uri_path /autodiscover/autodiscover.json** que contiene una de las siguientes cadenas **("powershell", "mapi/nspi", "mapi/emsmdb", "/EWS", "X-Rps)-CAT")** con el código de estado resultante 200, 301 o 302.

La actividad posterior a la explotación también se puede detectar mediante el análisis de:

- **Registros de PowerShell del servidor Exchange:**
    - El comando `New-ManagementRoleAssignment` indica que se otorgan privilegios de importación / exportación de buzones de correo.

   - El comando `New-MailboxExportRequest` es el indicativo de exportar el buzón de un usuario a una ruta UNC.
- **Registros de terminales del servidor Exchange:**
   - Proceso de creación de **MSExchangeMailboxReplication.exe**.
   - Proceso de creación de **powershell.exe** o **pwsh.exe** que contiene **New-MailboxExportRequest ***.

Recuerde que en caso de que detecte una explotación exitosa de su servidor, se debe realizar un análisis forense para determinar y revertir las acciones de los atacantes; puede reportar el incidente al CERT-PY, a abuse@cert.gov.py.

Soluciones:

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

- KB5001779 (Abril 2021)
- KB5003435 (Mayo 2021)

Información adicional:

- https://www.bleepingcomputer.com/news/microsoft/microsoft-exchange-servers-scanned-for-proxyshell-vulnerability-patch-now/
- https://www.blackhat.com/us-21/briefings/schedule/index.html#proxylogon-is-just-the-tip-of-the-iceberg-a-new-attack-surface-on-microsoft-exchange-server-23442
- https://davinsi.com/threat-advisory-how-to-respond-to-proxyshell-the-latest-exploit-against-exchange/