BOLETÍN DE ALERTA

Boletín Nro.: 2023-06
Fecha de publicación: 27/02/2023
Tema: Microsoft insta a eliminar algunas exclusiones de antivirus para Exchange on-premise

Software afectado:

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

Descripción:

Microsoft insta a los administradores a eliminar algunas exclusiones de antivirus recomendadas anteriormente para los servidores de correo Microsoft Exchange, con el fin mejorar la seguridad de los mismos.

Ejecutar programas antivirus de Windows en servidores de Microsoft Exchange puede ayudar a mejorar la seguridad de la organización, sin embargo, si no están configurados correctamente, los programas antivirus de Windows pueden causar problemas en Exchange Server.

Mantener estas exclusiones de antivirus recomendadas anteriormente por Microsoft, puede evitar la detección de *webshells* y módulos de *backdoor en el servidor de IIS*, así también se ha validado que la eliminación de estos procesos y carpetas no afecta el rendimiento o la estabilidad cuando se utiliza Microsoft Defender en Exchange Server 2019.

También se podría eliminar de forma segura estas exclusiones de los servidores que ejecutan Exchange Server 2016 y Exchange Server 2013, pero con una debida supervisión en caso de que se necesite mitigar cualquier problema que pueda surgir.

Las carpetas y procesos que deben ser eliminados de la exclusión del escaner del antivirus a nivel de archivo son:

```
%SystemRoot%\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files
%SystemRoot%\System32\Inetsrv
%SystemRoot%\System32\WindowsPowerShell\v1.0\PowerShell.exe
%SystemRoot%\System32\inetsrv\w3wp.exe
```

Impacto:

La exclusión de las carpetas mencionadas anteriormente del escáner del antivirus en Microsoft Exchange podría omitir la detección de archivos del tipo backdoors y webshells en el servidor web IIS de Microsoft Exchange on-premise, permitiendo a un atacante subir archivos maliciosos a estas carpetas mencionadas en el servidor web IIS.

Prevención:

- Se recomienda como medida de prevención mantener actualizados los servidores de Exchange. Utilizar soluciones de seguridad antimalware y/o antivirus reconocidos. Restringir el acceso a los *IIS virtual directories*, priorizar las alertas e inspeccionar regularmente los archivos de configuración y las carpetas *bin* en busca de archivos sospechosos.

- También se recomienda mantener actualizados los servidores Exchange locales, aplicando las actualizaciones acumulativas *(CU)* más reciente para tenerlos listos e implementar actualizaciones de seguridad de emergencia.

- Adicionalmente, también se recomienda ejecutar el *script* Comprobador de estado de Exchange Server después de implementar las actualizaciones para detectar problemas de configuración u otros problemas comunes.

Información adicional:

- https://www-bleepingcomputer-com.cdn.ampproject.org/c/s/www.bleepingcomputer.com/news/security/microsoft-urges-exchange-admins-to-remove-some-antivirus-exclusions/amp/
- https://techcommunity.microsoft.com/t5/exchange-team-blog/update-on-the-exchange-server-antivirus-exclusions/ba-p/3751464
- https://learn.microsoft.com/en-us/exchange/antispam-and-antimalware/windows-antivirus-software?view=exchserver-2019
- https://microsoft.github.io/CSS-Exchange/Diagnostics/HealthChecker/
- https://learn.microsoft.com/en-us/exchange/antispam-and-antimalware/windows-antivirus-software?view=exchserver-2019