BOLETÍN DE ALERTA

Boletín Nro.: 2022-02

Fecha de publicación: 13/01/2022

Tema: Vulnerabilidad de ejecución remota de código (RCE) en el protocolo HTTP de Windows.

Sistemas afectados:

- Microsoft Windows 10 versiones 1809 al 21H2.
- Microsoft Windows 11.
- Microsoft Windows Server versiones 2019 al 2022.

Descripción:

Microsoft ha publicado parches de seguridad dentro de su proceso normal de actualizaciones mensuales, para mitigar una vulnerabilidad de ejecución remota de código (RCE) que afectaría a sus distintos sistemas operativos.

Esta vulnerabilidad identificada como CVE-2022-21907, de severidad critica, con una puntuación de 9.8. Se debe a una mala configuración en la función *HTTP Protocol Stack,* que podría ser explotada enviando paquetes maliciosos al servidor objetivo.

Impacto:

Un atacante podría obtener control del sistema afectado a través de la ejecución remota de código (RCE).

Solución:

Recomendamos instalar las actualizaciones de seguridad correspondientes al sistema operativo utilizado de Windows mediante *Windows Update* indicado en la siguiente guía.

También Microsoft ha lanzado una mitigación adicional para las versiones de Windows Server 2019 y Windows 10 1809 la cual consiste en deshabilitar la funcionalidad *HTTP Trailer Support,* que por defecto se encuentra deshabilitado en el sistema, sin embargo si se encuentra habilitado como muestra a continuación podría el equipo ser vulnerable:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\HTTP\Parameters\

"EnableTrailerSupport"=dword:00000001

Si el registro se encuentra configurado de esta manera el *HTTP Trailer Support* está habilitado, para mitigarlo (deshabilitarlo) lo que debe hacer es borrar el valor del registro DWORD **"EnableTrailerSupport"** ubicado debajo de **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\HTTP\Parameters** .

Esto solamente aplica a los sistemas operativos mencionados anteriormente.

Información adicional:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21907#securityUpdates
- https://www.bleepingcomputer.com/news/microsoft/microsoft-new-critical-windows-http-vulnerability-is-wormable/
- https://nvd.nist.gov/vuln/detail/CVE-2022-21907
- https://vuldb.com/es/?id.190128
- https://securityonline.info/cve-2022-21907-http-protocol-stack-remote-code-execution-vulnerability/