BOLETÍN DE ALERTA

Boletín Nro.: 2021-12

Fecha de publicación: 21/05/2021

Tema: Vulnerabilidades críticas en productos de Microsoft

Sistemas y productos afectados:

- Microsoft Windows Server 2012, 2012 R2, 2016, 2019.
- Microsoft Windows 8, 8.1 (32 y 64 bits), 10 (32 y 64 bits).
- .NET Core & Visual Studio, HTTP.sys, Internet Explorer, Microsoft Accessibility Insights for Web, Microsoft Bluetooth Driver, Microsoft Dynamics Finance & Operations, Microsoft Exchange Server, Microsoft Graphics Component, Microsoft Office, Microsoft Office Access, Microsoft Office Excel, Microsoft Office SharePoint, Microsoft Office Word, Microsoft Windows Codecs Library, Microsoft Windows IrDA, Open Source Software, Role: Hyper-V, Skype for Business and Microsoft Lync, Visual Studio, Visual Studio Code, Windows Container Isolation FS Filter Driver, Windows Container Manager Service, Windows Cryptographic Services, Windows CSC Service, Windows Desktop Bridge, Windows OLE, Windows Projected File System FS Filter, Windows RDP Client, Windows SMB, Windows SSDP Service, Windows WalletService, Windows Wireless Networking.

Descripción:

Microsoft publicó 55 vulnerabilidades de seguridad en su Patch Tuesday mensual, incluyendo vulnerabilidades de ejecución remota de código (RCE) que representaron el 40% de las vulnerabilidades parcheadas este mes, seguidas de Elevation of Privilege (EoP) con un 20%.

Las vulnerabilidades abarcan una amplia gama de productos que en general incluyen parches para Microsoft Windows, Internet Explorer (IE), Microsoft Exchange Server, Microsoft Office, .NET Core y Visual Studio, SharePoint Server, Hyper-V, software de código abierto, Skype for Business y Microsoft Lync.

De las 55 CVE parcheadas por Microsoft en el Patch Tuesday de mayo 4 son clasificadas como Críticas, 50 clasificadas como Importantes y 1 como Moderada. Puede encontrar una lista completa de todas las vulnerabilidades en el siguiente enlace: https://msrc.microsoft.com/update-guide/en-us.

Vulnerabilidades críticas:

- CVE-2021-31166 de severidad crítica con una puntuación de 9.8. Vulnerabilidad de ejecución remota de código de pila de protocolo HTTP, este error podría permitir que un atacante no autenticado ejecute código como kernel de forma remota. Un atacante simplemente necesitaría enviar un paquete especialmente diseñado a un servidor afectado. Esta vulnerabilidad es especialmente crítica ya que se trata de un módulo de IIS, el cual normalmente se encuentra expuesto a Internet.
- CVE-2021-28476 de severidad crítica con una puntuación de 9.9. Vulnerabilidad de ejecución remota de código de Hyper-V. La vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el sistema de destino, debido a una validación de entrada incorrecta en Hyper-V. La explotación exitosa de esta vulnerabilidad puede resultar en un compromiso completo del sistema vulnerable.
- CVE-2021-27068 de severidad alta con una puntuación de 8.8. Vulnerabilidad de ejecución remota de código de Visual Studio, este error en Visual Studio 2019 podría permitir la ejecución de código arbitrario en el sistema de destino.
- CVE-2021-26419 de severidad alta con una puntuación de 7.5. Vulnerabilidad de corrupción de memoria en Scripting Engine, un error de corrupción de memoria del motor de secuencias de comandos que afecta a IE11. Para aprovechar el error, un usuario tendría que visitar un sitio web controlado por un atacante, aunque también podría activarse al insertar controles ActiveX en los documentos de Office.

Día Cero (Zero Day):

- CVE-2021-31207 Vulnerabilidad de omisión de la función de seguridad de Microsoft Exchange Server.
- CVE-2021-31200 Ejecución remota de código de utilidades comunes en Common Utilities.
- CVE-2021-31204 Vulnerabilidad de elevación de privilegios de .NET y Visual Studio.

Otras vulnerabilidades importantes parcheadas:

- CVE-2021-31188 y CVE-2021-31170 Son fallas de escalamiento de privilegios locales que existen en el componente de gráficos de Windows.
- CVE-2021-31181 Vulnerabilidad de ejecución remota de código de SharePoint.
- CVE-2020-24589 Vulnerabilidad de divulgación de información de redes inalámbricas de Windows.
- CVE-2021-27068 Vulnerabilidad de ejecución remota de código de Visual Studio.
- CVE-2021-28476 Vulnerabilidad de ejecución remota de código de Hyper-V.

Impacto:

La explotación exitosa de las vulnerabilidades tienen diversos impactos, que van desde la ejecución remota de código y control total del servidor por parte de un atacante remoto, hasta la consecuencia de que un atacante obtenga los mismos privilegios que el usuario que inició sesión. Dependiendo de los privilegios asociados con el usuario, un atacante podría instalar programas; ver, cambiar o eliminar datos; o crear nuevas cuentas con todos los derechos de usuario.

Solución:

- Aplique los parches apropiados o las mitigaciones adecuadas proporcionadas por Microsoft a los sistemas vulnerables inmediatamente.
- Los usuarios que tengan instalados Windows 7, Windows Server 2008 R2 o Windows Server 2008 necesitan adquirir el Extended Security Update para recibir las actualizaciones de seguridad.

Prevención:

- Ejecute todo el software como un usuario con los menores privilegios necesarios (uno sin derechos administrativos) para disminuir los efectos de un ataque exitoso.

- Recuerde a los usuarios de sus sistemas que no deben visitar sitios web que no sean de confianza ni seguir enlaces proporcionados por fuentes desconocidas o que no sean de confianza.
- Informar y educar a los usuarios sobre las amenazas planteadas por los enlaces de hipertexto contenidos en correos electrónicos o archivos adjuntos, especialmente de fuentes no confiables.
- Aplicar el principio de privilegio mínimo a todos los sistemas y servicios.

Información adicional:

- https://msrc.microsoft.com/update-guide/en-us
- https://blog.ehcgroup.io/2021/05/11/13/21/35/11106/martes-de-parche-de-mayo-de-2021-de-microsoft-corrige-55-fallas-3-zero-days/noticias-de-seguridad/ehacking/
- https://www.welivesecurity.com/la-es/2021/05/12/actualizacion-seguridad-microsoft-mayo-corrige-tres-zero-day/
- https://portal.cci-entel.cl/Threat_Intelligence/Boletines/889/