Microsoft publicó actualizaciones de seguridad como parte de su ciclo de lanzamiento mensual del martes de parches para abordar 55 vulnerabilidades en Windows, Azure, Visual Studio, Windows Hyper-V y Office, incluyendo correcciones para dos vulnerabilidades de día cero explotadas activamente en Excel y Exchange Server que podría abusarse para tomar el control de un sistema afectado.

De las 55 vulnerabilidades, 6 están calificadas como críticas y 49 como importantes en gravedad, otras cuatro figuran como conocidas públicamente al momento del lanzamiento.

Las vulnerabilidades más críticas son CVE-2021-42321 con puntuación CVSS de 8.8 y CVE-2021-42292 con puntuación CVSS de 7.8, cada una relacionada con una falla de ejecución remota de código posterior a la autenticación en Microsoft Exchange Server y una vulnerabilidad de omisión de seguridad, impactando las versiones 2013-2021 de Microsoft Excel respectivamente.

El problema de Exchange Server es también uno de los errores que se demostró en la Copa Tianfu, celebrada en China el mes pasado. Sin embargo, la compañía con sede en Redmond no proporcionó ningún detalle sobre cómo se utilizaron las dos vulnerabilidades mencionadas anteriormente en ataques en el mundo real.

> *«A inicios del año, Microsoft alertó que el grupo APT HAFNIUM estaba explotando cuatro vulnerabilidades de día cero en el servidor Microsoft Exchange»,* dijo Bharat Jogi, director de investigación de vulnerabilidades y amenazas de Qualys.
>
> *«Esto se convirtió en explotaciones de las vulnerabilidades del servidor Exchange por parte de DearCry Ransomware, incluidos los ataques a investigadores de enfermedades infecciosas, bufetes de abogados, universidades, contratistas de defensa, grupos de expertos en políticas y ONG. Ejemplos como estos subrayan aún más que los servidores de Microsoft Exchange son objetivos de gran valor para hackers que buscan penetrar en redes críticas»,* agregó Jogi.

También se abordan cuatro vulnerabilidades divulgadas públicamente, pero no explotadas:

- CVE-2021-43208 con puntuación CVSS de 7.8: Vulnerabilidad de ejecución remota de código del visor 3D
- CVE-2021-43209 con puntuación CVSS de 7.8: Vulnerabilidad de ejecución remota de código del visor 3D
- CVE-2021-38631 con puntuación CVSS de 4.4: Vulnerabilidad de divulgación de información del Protocolo de Escritorio Remoto de Windows (RDP)
- CVE-2021-41371 con puntuación CVSS de 4.4: Vulnerabilidad de divulgación de información del Protocolo de Escritorio Remoto de Windows (RDP)

El parche de noviembre de Microsoft también cuenta con una resolución para CVE-2021-3711, una falla crítica de desbordamiento de búfer en la función de descifrado SM2 de OpenSSL, que salió a la luz a fines de agosto de 2021 y podría ser abusada por adversarios para ejecutar código arbitrario y causar una denegación de condición de servicio (DoS).

Otras correcciones importantes se incluyen para vulnerabilidades de ejecución de código remoto en Chakra Scripting Engine (CVE-2021-42279), Microsoft Defender (CVE-2021-42298), Microsoft Virtual Machine Bus (CVE-2021-26443), Cliente de Escritorio Remoto (CVE-2021-38666) y versiones locales de Microsoft Dynamics 365 (CVE-2021-42316).

Finalmente, la actualización se completa con parches para una serie de vulnerabilidades de escalada de privilegios que afectan a NTFS (CVE-2021-41367, CVE-2021-41370, CVE-2021-42283), Windows Kernel (CVE-2021-42285), Visual Studio Code (CVE-2021-42322), Puente de Escritorio de Windows (CVE-2021-36957) y Controlador del sistema de archivos Fast FAT de Windows (CVE-2021-41377).