Microsoft emitió este martes correcciones para 56 vulnerabilidades, incluida una falla crítica que está siendo explotada activamente en la naturaleza.

En total, 11 vulnerabilidades se calificaron como críticas, 43 importantes y dos como moderadas, seis de las cuales ya fueron divulgadas anteriormente.

Las actualizaciones cubren .NET Framework, Azure IoT, Microsoft Dynamics, Microsoft Edge para Android, Microsoft Exchange Server, Microsoft Office, Microsoft Windows Codecs Library, Skype for Business, Visual Studio, Windows Defender y otros componentes centrales como Kernel, TCP/IP, cola de impresión y llamada a procedimiento remoto (RPC).

La falla más crítica es una vulnerabilidad de escalada de privilegios de Windows Win32k (CVE-2021-1732, con puntuación CVSS de 7.8), que permite a los atacantes con acceso a un sistema de destino ejecutar código malicioso con permisos elevados. Microsoft brindó crédito a JinQuan, MaDongZe, TuXiao y LiHao de DBAPPSecurity por descubrir y reportar la vulnerabilidad.

En un artículo técnico separado, los investigadores dijeron que se detectó un exploit de día cero que aprovecha la falla en un *«número muy limitado de ataques»* contra víctimas ubicadas en China por un actor de amenazas llamado Bitter APT. Los ataques fueron descubiertos en diciembre de 2020.

> *«Este día cero es una nueva vulnerabilidad que se causó por devolución de llamada win32k, que podría ser utilizado para escapar de la sandbox del navegador Internet Explorer o Adobe Reader en la última versión de Windows 10. La vulnerabilidad es de alta calidad y el exploit es sofisticado»*, dijo DBAPPSecurity.

Cabe mencionar que Adobe, como parte de su parche de febrero, abordó una falla crítica de desbordamiento de búfer en Adobe Acrobat Reader para Windows y macOS (CVE-2021-21017) que, según la compañía, podría conducir a la ejecución de código arbitrario en el contexto del usuario actual.

La compañía también advirtió sobre intentos de explotación activa contra la vulnerabilidad en la naturaleza en ataques limitados dirigidos a usuarios de Adobe Reader en Windows, reflejando los hallazgos antes mencionados de DBAPPSecurity.

Aunque ni Microsoft ni Adobe proporcionaron detalles adicionales, el parcheo simultáneo de las dos vulnerabilidades podría indicar que ambas estén encadenadas para llevar a cabo los ataques.

La actualización Patch Tuesday de Microsoft para febrero de 2021 resuelve una serie de vulnerabilidades de ejecución remota de código (RCE) en Windows DNS Server (CVE-2021-24078), .NET Core y Visual Studio (CVE-2021-26701), Microsoft Windows Codecs Library (CVE-2021-24081) y Servicio de Fax (CVE-2021-1722 y CVE-2021-24077).

El RCE en el componente de DNS Server de Windows tiene una calificación de 9.8 en gravedad, lo que lo convierte en una vulnerabilidad crítica que de no ser corregida, podría permitir que un atacante ejecute código arbitrario y redirija potencialmente el tráfico legítimo a servidores maliciosos.

Microsoft también tomó este mes para impulsar la segunda ronda de correcciones para la falla de Zerologon (CVE-2020-1472), que se resolvió originalmente en agosto de 2020, luego de lo cual surgieron informes de explotación activa dirigida a sistemas sin parches en septiembre de 2020.

A partir del 9 de febrero, el *«modo de aplicación»* del controlador de dominio estará habilitado de forma predeterminada, bloqueando de este modo las *«conexiones vulnerables de dispositivos no compatibles».*

Además, la actualización Patch Tuesday rectifica un error en el navegador Edge para Android (CVE-2021-24100) que podría revelar información de identificación personal e información de pago de un usuario.

Por último, Microsoft lanzó un conjunto de correcciones que afectan su implementación de

TCP/IP, que consta de dos vulnerabilidades de RCE (CVE-2021-24074 y CVE-2021-24094) y una vulnerabilidad de denegación de servicio (CVE-2021-24086), que dijo que podría aprovecharse con un ataque DoS.

> *«Los exploits DoS para estos CVE permitirían que un atacante remoto provocara un error de detención. Los clientes pueden recibir una pantalla azul en cualquier sistema Windows que esté directamente expuesto a Internet con un tráfico de red mínimo. Por lo tanto, recomendamos a los clientes que se apresuren a aplicar las actualizaciones de seguridad de Windows este mes»*, dijo Microsoft.

Sin embargo, la compañía señaló que la complejidad de las dos vulnerabilidades de TCP/IP RCE dificultaría el desarrollo de exploits funcionales. Pero espera que los atacantes realicen ataques DoS con mucha más facilidad, convirtiendo la falla de seguridad en un candidato ideal para la explotación en la naturaleza.