Microsoft publicó hoy actualizaciones de seguridad, al igual que otras compañías como Adobe.

En esta ocasión, Microsoft liberó actualizaciones de software para un total de 79 vulnerabilidades enumeradas en CVE en sus sistemas operativos Windows y otros productos, incluido un defecto de gusano crítico que puede propagar malware de computadora a computadora sin tener que interactuar con los usuarios.

De las 79 vulnerabilidades, 18 problemas fueron calificados como críticos e importantes. Dos de las vulnerabilidades tratadas este mes se enumeran como conocidas públicamente, de las cuales una se encuentra bajo ataque activo en el momento del lanzamiento.

Las actualizaciones de seguridad de mayo de 2019 solucionan fallas en el sistema operativo Windows, Internet Explorer, Edge, Microsoft Office y Microsoft Office Services y aplicaciones web, ChakraCore, .NET Framework y ASP.NET, Skype para Android, Azure DevOps Server y el administrador de paquetes NuGet.

Vulnerabilidad RDP de gusano crítico

La vulnerabilidad de gusano (CVE-2019-0708) reside en los servicios de escritorio remoto, anteriormente conocidos como Servicios de Terminal, que podrían explotarse de forma remota mediante el envío de solicitudes especialmente diseñadas por medio de un protocolo RDP a un sistema específico.

La vulnerabilidad podría ser explotada para propagar malware extraíble de forma similar a como el malware WannaCry se extendió por todo el mundo en 2017.

> *«Esta vulnerabilidad es una autenticación previa y no requiere la interacción del usuario. Un atacante que aprovechó esta vulnerabilidad podría ejecutar un código arbitrario en el sistema de destino. Si bien no hemos observado ninguna explotación de esta vulnerabilidad, es muy probable que los actores*

> *malintencionados escriban un exploit para esta vulnerabilidad la incorporen en su malware»,* escribió Microsoft.

Además de lanzar parches para los sistemas compatibles, incluyendo Windows 7, Windows Server 2008 R2 y Windows Server 2008, Microsoft también lanzó correcciones por separado para las versones de Windows sin soporte, incluidas Windows 2003 y Windows XP, para dar solución a este problema crítico.

Como solución alternativa, Microsoft aconsejó a los usuarios de Windows Server que bloqueen el puerto TCP 3389 y habiliten la autenticación de nivel de red para evitar que cualquier atacante aproveche esta falla.

Otras vulnerabilidades críticas

Otra falla grave es una vulnerabilidad de elevación de privilegios (CVE-2019-0863) en Windows, que existe en la forma en que Windows Error Reporting (WER) maneja los archivos. La falla está listada como públicamente conocida y ya está siendo explotada activamente en ataques limitados contra objetivos específicos.

La explotación exitosa de la falla podría permitir que un atacante remoto con pocos privilegios ejecute código arbitrario en el modo kernel con privilegios de administrador, lo que eventualmente les permitirá instalar programas, ver, cambiar o eliminar datos, o crear nuevas cuentas con privilegios de administrador.

Otra vulnerabilidad divulgada públicamente afecta a la aplicación de Skype para Android. La vulnerabilidad (CVE-2019-0932) podría permitir a un atacante escuchar la conversación de los usuarios de Skype sin su conocimiento.

Para aprovechar exitosamente esta vulnerabilidad, todo lo que necesita un atacante es llamar a un teléfono Android con Skype para Android instalado que también está emparejando con un dispositivo Bluetooth.

Todas las vulnerabilidades críticas enumeradas este mes afectan principalmente a varias versiones del sistema operativo Windows 10 y las ediciones de Server, principalmente residen en Chakra Scriptong Engine, y algunas también residen en la Interfaz de dispositivo de gráficos de Windows (GDI), Internet Explorer, Edge, Word, Servicios de escritorio remoto y el servidor DHCP de Windows.

Muchas vulnerabilidades calificadas como importantes también conducen a ataques de ejecución remota de código, mientras que otras permiten la elevación de privilegios, la divulgación de información, desvío de seguridad, manipulación falsa y los ataques de denegación de servicio.

Se recomienda a los usuarios y administradores de sistema que apliquen los últimos parches de seguridad lo antes posible para evitar que los ciberdelincuentes y piratas informáticos tomen el control de las computadoras.