Microsoft lanzó hoy su lote de actualizaciones de seguridad de junio de 2020, que parchea 129 vulnerabilidades recientemente descubiertas que afectan a distintas versiones de los sistemas operativos Windows y otros productos de la compañía.

Los 129 defectos en el paquete de junio de 2020 para administradores de sistemas y miles de millones de usuarios, incluyen 11 vulnerabilidades críticas, que conducen a ataques de ejecución remota de código, 118 clasificadas como importantes en grado de severidad, principalmente conducen a escalada de privilegios y ataques de suplantación de identidad.

Según las advertencias de Microsoft, los hackers no han explotado ninguna de las vulnerabilidades de día cero, y los detalles de los defectos abordados este mes no han sido divulgados públicamente.

Una de las vulnerabilidades notables conlleva la divulgación de información (CVE-2020-1206), en el protocolo Server Message Block 3.1.1 (SMBv2) que, según un equipo de investigadores, puede explotarse en combinación con SMBGhost (CVE-2020-0796) para realizar ataques de ejecución remota de código.

Por otro lado, tres vulnerabilidades críticas (CVE-2020-1213, CVE-2020-1216 y CVE-2020-1260), afectan el motor VBScript y existen en la forma en que se manejan los objetos en la memoria, lo que permite a un atacante ejecutar código arbitrario en el contexto del usuario actual.

Microsoft enumeró las fallas como *«más probable de explotación»,* afirmando que ha visto atacantes explotar consistentemente fallas similares en el pasado, y puede llevarse a cabo de forma remota por medio del navegador, la aplicación o el documento de Microsoft Office que aloja el motor de renderizado IE.

Uno de los 11 problemas críticos explota una vulnerabilidad (CVE-2020-1299) en la forma en que Windows maneja los archivos de acceso directo (.LNK), lo que permite a los atacantes ejecutar código arbitrario en los sistemas de forma remota. Como todas las vulnerabilidades anteriores de LNK, este tipo de ataque también podría llevar a las víctimas a perder el control

de sus computadoras o que les roben sus datos confidenciales.

El componente GDI+ que permite a los programas usar gráficos y texto formateado en una pantalla de video o impresora en Windows, también se ha encontrado vulnerable a un error de ejecución remota de código (CVE-2020-1248).

Según Microsoft, la vulnerabilidad GDI+RCE puede explotarse en combinación con otra vulnerabilidad crítica separada (CVE-2020-1229) que afecta al software Microsoft Outlook, y podría permitir a los hackers cargar automáticamente imágenes maliciosas alojadas en un servidor remoto.

> *«En un escenario de ataque por correo electrónico, un atacante podría explotar la vulnerabilidad enviando la imagen especialmente diseñada al usuario. Un atacante que explote con éxito esta vulnerabilidad, podría hacer que un sistema cargue imágenes remotas. Estas imágenes podrían revelar la dirección IP del sistema objetivo al atacante»*, dice el aviso de Microsoft.

Además, la actualización de junio de 2020 también incluye un parche para un nuevo error crítico de ejecución remota de código (CVE-2020-9633) que afecta a Adobe Flash Player para sistemas Windows.

Se recomienda que todos los usuarios apliquen los últimos parches de seguridad lo antes posible para evitar que el malware o los hackers los exploten para obtener control remoto sobre computadoras vulnerables.