Microsoft lanzó ayer sus actualizaciones de seguridad del martes del mes de octubre de 2019, para abordar un total de 59 vulnerabilidades en los sistemas operativos Windows y software relacionado, de las cuales, 9 son críticas, 49 importantes y una de gravedad moderada.

En esta ocasión, después de mucho tiempo, ninguna de las vulnerabilidades de seguridad parcheadas por Microsoft aparece como públicamente conocida o bajo ataques activos.

Además, no existe un parche acumulativo para Adobe Flash Player incluido en la actualización de Windows para este mes. Microsoft también publicó un aviso recordatorio para los usuarios de Windows 7 y Windows Server 2008 R2, advirtiendo que el soporte extendido para estos sistemas operativos, está apunto de finalizar en los próximos dos meses y que ya no recibirán actualizaciones a partir del 14 de enero de 2020.

En el caso de las vulnerabilidades críticas, dos de estas son fallas de ejecución remota de código en el motor VBScript, y ambas existen en la forma en que VBScript maneja los objetos en la memoria, permitiendo a los atacantes corromper la memoria y ejecutar código arbitrario en el contexto del usuario actual.

Estas dos vulnerabilidades, identificadas como CVE-2019-1238 y CVE-2019-1239, pueden explotarse de forma remota engañando a las víctimas para que visiten un sitio web especialmente diseñado por medio de Internet Explorer.

Un atacante también puede expotar estos problemas utilizando una aplicación o documento de Microsoft Office al incorporar un control AciveX marcado como *«seguro para la inicialización»* que utiliza el motor de renderizado de Internet Explorer.

Al igual que en los últimos meses, Microsoft ha parcheado otro ataque RDP inverso, donde los atacantes pueden tomar el control de las computadoras cliente que se conectan a un servidor RDP malicioso explotando una vulnerabilidad crítica de ejecución remota de código en la aplicación de cliente de escritorio remoto incorporada de Windows.

A diferencia de la vulnerabilidad de BlueKeep, que se puede parchear, la vulnerabilidad RDP recién parcheada es del lado del cliente, lo que requiere que un atacante engañe a las víctimas para que se conecten a un servidor RDP malicioso por medio de ingeniería social, envenenamiento de DNS o utilizando una técnica Man in the Middle (MITM).

Tres vulnerabilidades críticas de RCE son fallas de corrupción de memoria en la forma en que el motor de secuencias de comandos de Chakra maneja objetos en la memoria en Microsoft Edge, mientras que una falla crítica de RCE es un problema de elevación de privilegios que existe cuando Azure App Service en Azure Stack no puede verificar la longitud de un buffer antes de copiarle memoria.

Otras vulnerabilidades parcheadas por Microsoft este mes y marcadas como importantes, residen en los siguientes productos y servicios:

- Microsoft Windows
- Microsoft Edge
- Internet Explorer
- ChakraCore
- Microsoft Office, Office Services and Web Apps
- SQL Server Management Studio
- Open Source Software
- Microsoft Dynamics 365
- Windows Update Assistant

La mayoría de estas vulnerabilidades permiten la elevación de privilegios, y algunas también conducen a ataques de ejecución remota de código, mientras que otras permiten la divulgación de información, secuencias de comandos entre sitios (XSS), omisión de características de seguridad, suplantación de identidad, manipulación y ataques de denegación de servicio.

Se recomienda a los usuarios de Windows a los administradores de sistemas, que apliquen los últimos parches de seguridad lo antes posible para evitar que los hackers tomen el

control de las computadoras.