Microsoft implementó parches de seguridad de emergencia fuera de banda para dos nuevas vulnerabilidades, una de las cuales es un 0-Day crítico de Internet Explorer que los ciberdelincuentes están explotando activamente.

Descubierto por Clément Lecigne, del Grupo de Análisis de Amenazas de Google, y rastreado como CVE-2019-1367, el día cero de IE es una vulnerabilidad de ejecución remota de código en la forma en que el motor de secuencias de comandos de Microsoft maneja los objetos en la memoria en Internet Explorer.

La vulnerabilidad es un problema de corrupción de memoria que podría permitir a un hacker remoto secuestrar una PC con Windows simplemente al convencer al usuario de que vea una página web especialmente diseñada y atrapada alojada en línea, cuando se utiliza Internet Explorer.

> *«Un atacante que explotó con éxito esta vulnerabilidad podría obtener los mismos derechos de usuario que el usuario actual. Si el usuario actual inicia sesión con derechos de usuario administrativos, un atacante que explotó con éxito la vulnerabilidad podría tomar el control de un sistema afectado»,* dijo Microsoft.

La vulnerabilidad afecta a las versiones 9, 10 y 11 de Internet Explorer, y aunque los usuarios siempre deben implementar actualizaciones para cada software instalado cuando esté disponible, se recomienda utilizar un navegador web alternativo y más seguro como Google Chrome o Mozilla Firefox.

Microsoft dijo que esta vulnerabilidad está siendo explotada activamente en la naturaleza por lo atacantes, pero no reveló más detalles sobre la campaña.

Google también detectó recientemente una campaña generalizada de piratería de iPhone que se dirigió indiscriminadamente a los usuarios por más de dos años, pero Apple acusó a la compañía de tecnología de crear una falsa impresión de *«explotación masiva».*

Microsoft también lanzó una segunda actualización de seguridad fuera de banda para parchear una vulnerabilidad de denegación de servicio (DoS) en Microsoft Defender, un motor antimalware que se entrega con Windows 8 y versiones posteriores del sistema operativo Windows.

Descubierta por Charalampos Billinis, de F-Secure y Wenxu Wu, de Tencent Security Lab, y rastreada como CVE-2019-1255, la vulnerabilidad reside en la forma en que Microsoft Defender maneja los archivos y existe en las versiones de Microsoft Malware Protection Engine hasta 1.1.16300.1.

Según un aviso publicado por Microsoft, un atacante sería capaz de explotar dicha vulnerabilidad *«para evitar que cuentas legítimas ejecuten archivos binarios legítimos del sistema»,* pero para explotar la falla, el atacante *«primero requeriría la ejecución en el sistema de la víctima».*

La actualización de seguridad para Microsoft Defender es automática, por lo que se aplicará a través del motor de protección contra Malware de Microsoft en las siguientes 48 horas. La falla se solucionó en el motor de protección contra malware de Microsoft versión 1.1.16400.2.

Debido a que ambas actualizaciones de seguridad son parte de las actualizaciones de emergencia de Microsoft y una de ellas incluso, aborda la falla que se explota activamente en este momento, se recomienda que se implementen lo antes posible.