Microsoft publicó hoy un aviso de seguridad sobre una vulnerabilidad de día cero de Internet Explorer (IE) que actualmente está siendo explotada en la naturaleza.

El aviso de seguridad, identificado como ADV200001, actualmente solo incluye soluciones y mitigaciones que se pueden aplicar para proteger los sistemas vulnerables de los ataques.

Hasta ahora no existe parche para el problema. Microsoft informó que está trabajando en una solución y que el parche se lanzará en una fecha futura.

Aunque Microsoft dijo que sabía que el 0-day de IE estaba siendo explotado en la naturaleza, la compañía describió estos como *«ataques dirigidos limitados»*, sugiriendo que el día cero no fue ampliamente explotado, sino que era parte de los ataques dirigidos a un número pequeño de usuarios.

Se cree que dichos ataques de día cero de IE son parte de una campaña de piratería más grande, que también implica ataques contra usuarios de Mozilla Firefox.

La semana pasada, Mozilla parchó una vulnerabilidad Zero Day parecida, que estaba siendo explotada para atacar a los usuarios de Firefox. Mozilla acreditó a Qihoo 360 el descubrimiento de la vulnerabilidad.

RCE en Internet Explorer

Técnicamente, Microsoft describió el 0-day como un error de ejecución remota de código (RCE), causado por un error de corrupción de memoria en el motor de secuencias de comandos de IE, el componente del navegador que maneja el código JavaScript.

> *«Existe una vulnerabilidad de ejecución remota de código en la forma en que el motor de secuencias de comandos maneja los objetos en la memoria en Internet Explorer. La vulnerabilidad podría corromper la memoria de tal forma que un hacker podría ejecutar código arbitrario en el contexto del usuario actual. Un atacante que*

> *aproveche la vulnerabilidad con éxito podría obtener los mismos derechos de usuario que el usuario actual. Si el usuario actual ha iniciado sesión con derechos de usuario administrativos, un atacante que haya explotado con éxito la vulnerabilidad podría tomar el control de un sistema afectado. Un atacante podría instalar programas, ver, cambiar o eliminar datos, o crear nuevas cuentas con plenos derechos de usuario»,* dice la descripción de Microsoft.

Microsoft también dijo que todas las versiones compatibles de escritorio de Windows y SO de servidor se ven afectadas. El día cero de IE no tiene un identificador CVE por el momento.

La compañía parcheó dos 0-day de IE similares en septiembre y noviembre de 2019. Aunque IE ya no es el navegador predeterminado en las últimas versiones de Windows, el navegador sigue siendo incluido en los sistemas operativos Windows, y muchas empresas siguen utilizándolo por temas de compatibilidad.