JasBug, La Vulnerabilidad En Windows Que Afecta A Todas Las Versiones

Microsoft acaba de publicar un parche crítico para corregir una **vulnerabilidad en Windows**, la cual ha estado presente durante 15 años. Esta vulnerabilidad podría ser usada para secuestrar remotamente los PCs de los usuarios, sin importar cual sea la versión de Windows.

La vulnerabilidad crítica ha sido nombrada como «**JASBUG**» por el investigador que informó del fallo, se debe a un defecto en el diseño fundamental de Windows, el cual Microsoft tomó más de 12 meses para liberar una solución. Sin embargo, la falla está todavía **sin solucionar en Windows Server 2003**, dejando la versión expuesta a los hackers.

Fácilmente Pueden Tomar El Control De Tu Equipo

La vulnerabilidad (CVE-2.015-0008) podría permitir a un atacante secuestrar fácilmente un sistema de dominio de Windows configurado si está conectado a una red maliciosa, ya sea de forma inalámbrica o cableada, dar su consentimiento atacante para hacer varias tareas, incluyendo, instalar programas; eliminar, alterar o examinar los datos de los usuarios; o crear cuentas nuevas con todos los derechos de usuario.

Sin embargo, la **vulnerabilidad Jasbug** no afecta a los usuarios domésticos, ya que no suelen ser de dominio configurado, pero el error es una molestia enorme para **profesionales de TI** que normalmente se conectan a las redes de negocio, corporativas, de gobierno o utilizando el servicio de Active Directory.

Versiones De Windows Afectadas Por JasBug

- Windows Vista
- Windows 7
- Windows 8
- Windows RT
- Windows 8.1
- Windows RT 8.1
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

¿Como Funciona JasBug?

Microsoft, en su entrada del blog, proporciona el siguiente ejemplo de cómo un hacker malicioso podría aprovechar esta vulnerabilidad JasBug en una máquina conectada a través de Wi-Fi abierta en una cafetería:

- Este es un ejemplo de un escenario de un ataque en la «cafetería», donde un atacante intentaría realizar cambios en un Switch de red compartida, en un lugar público y poder dirigir el tráfico de los clientes a un sistema controlado por el atacante.
- En este escenario, el atacante ha observado tráfico a través del Switch y encontró que una máquina específica está intentando descargar un archivo ubicado en la ruta de acceso UNC: **\\10.0.0.100\Share\Login.bat**.
- En el equipo del atacante, una acción se estableció que coincide exactamente con la ruta UNC del archivo solicitado por la víctima: *\Share\Login.bat.
- El atacante modifica la tabla ARP en el Switch local para asegurar que el tráfico destinado al servidor de

destino 10.0.0.100 está enrutado a través de la máquina del atacante.

- Cuando la máquina de la víctima solicita el archivo, la máquina del atacante retornará la versión maliciosa de **login.bat**. Este escenario también ilustra que este ataque no se puede utilizar ampliamente a través de Internet, un atacante necesita llegar a un sistema o grupo de sistemas que solicitan archivos con rutas UNC.

También existen dos **vulnerabilidades en Microsoft Office**, las cuales podrían permitir RCE y la función de la seguridad Bypass, y los errores en Windows que podría permitir la elevación de privilegios, característica de seguridad de derivación y divulgación de información. También hay una vulnerabilidad en Virtual Machine Manager (VMM), la cual daría a un atacante privilegios elevados.