Los parches de mayo de Microsoft arreglan 2 vulnerabilidades zero-day

Microsoft ha publicado su paquete mensual de parches de seguridad. Los Parches del Martes correspondientes al mes de mayo corrigen un total de 67 vulnerabilidades halladas en los distintos productos del gigante de Redmond, abarcando Internet Explorer, Microsoft Edge, Windows, y Office, a lo que hay que sumar una actualización para Adobe Flash Player.

De todos los fallos de seguridad parcheados, 21 han sido considerados como críticos, 45 como importantes, 2 como leves, 32 permitían la ejecución de código en remoto y 2 de ellos eran zero-day. De todas vulnerabilidades, Microsoft destaca la CVE-2018-8174 (la primera zero-day), que permitía la ejecución de código en remoto en caso de que la víctima visitase un

sitio web malicioso controlado por el atacante. Además, este problema de seguridad también puede ser usado junto a un control de ActiveX malicioso marcado como “seguro para iniciarse” en una aplicación, un documento de MS Office o dentro del motor de renderizado de Internet Explorer.

El segundo fallo de seguridad zero-day destacado (CVE-2018-8120) es un exploit activo que permitía realizar una elevación de privilegios, la cual impactaba en el componente Win32k de Windows. En caso de ser explotada con éxito, permitía (y permite en caso de no aplicarse el parche) a un atacante ejecutar código arbitrario en el modo kernel de Windows. Desde ahí se podía obtener control sobre partes importantes del sistema operativo, pudiendo instalar programas; ver, cambiar y modificar datos; y crear cuentas con privilegios de administración. El fallo afectaba a Windows y Server 2008 R2. Los atacantes suelen apoyarse en Win32k para evitar los mecanismos de aislamiento.

El hipervisor Hyper-V también ha recibido actualizaciones para corregir fallos de seguridad hallados en él. Concretamente, se han encontrado dos: Uno (CVE-2018-0961) permitía abusar de los que paquetes de vSMB, mientras que otro (CVE-2018-0959) hacía posible la ejecución de código abritrario sobre el anfitrión desde un sistema operativo invitado. Otra vulnerabilidad, esta contra el modo kernel en Windows 10 y Windows Server 1709 (CVE-2018-8141), abría la puerta a la divulgación de información para que un atacante pudiera obtener información adicional para comprometer el sistema. En los mismos Windows 10 y Windows Server 1709 se ha encontrado otra vulnerabilidad de elevación de privilegios (CVE-2018-8170).

Fuente: muyseguridad.