TECNOLOGÍA | SEGURIDAD INFORMÁTICA

**El “parche” de Microsoft de este mes corrige varios fallos de seguridad**

*Microsoft ha abordado una vulnerabilidad de escalada de privilegios en el controlador de kernel Win32k, permitiendo a los atacantes elevar sus privilegios a SYSTEM, el nivel de privilegio de usuario más alto en Windows.*

**Por Julián M. Zappia.  
Diplomatic Week.**

Como parte de sus actualizaciones regulares de “Patch Tuesday”, Microsoft ha lanzado su paquete de seguridad para este mes, resolviendo un total de 38 vulnerabilidades de seguridad en sus diversos productos.

La compañía ha corregido vulnerabilidades de día cero, dos de ellas explotadas activamente en ataques, mientras que la tercera se divulgó públicamente. Microsoft clasifica un fallo de seguridad como de día cero si se explota activamente o se divulga públicamente, y no existe una solución oficial para él.

De las 38 vulnerabilidades abordadas este mes, seis se califican como “críticas”, y las 32 restantes como “importantes” en severidad. Ocho han sido marcadas con una evaluación de “explotación más Probable por Microsoft.

Además, Microsoft también ha abordado 11 fallos en su navegador basado en Chromium, Edge, desde principios de este mes.

**Continúan las soluciones.**

Actualmente, hay dos vulnerabilidades que se están explotando activamente. Una de ellas es CVE-2023-24932, una falla de bypass de Secure Boot que ha sido utilizada por un actor de amenazas para instalar el bootkit BlackLotus UEFI.

El bootkit BlackLotus es capaz de eludir esta medida de seguridad explotando debilidades en el proceso de arranque.

Esto permite que el bootkit se cargue antes que cualquier otra cosa, incluyendo el sistema operativo y cualquier herramienta de seguridad que potencialmente podría prevenir su ejecución.

Una vez instalado, el bootkit BlackLotus puede desactivar las defensas antivirus e instalar un controlador de kernel que puede recibir comandos de un servidor de control.

Ell asesoramiento de Microsoft dice “para explotar la vulnerabilidad, un atacante que tiene acceso físico o derechos administrativos a un dispositivo objetivo podría instalar una política de arranque afectada”.

Microsoft también ha abordado una vulnerabilidad de escalada de privilegios (CVE-2023-29336) en el controlador de kernel Win32k, que permite a los atacantes elevar sus privilegios a SYSTEM, el nivel de privilegio de usuario más alto en Windows.

Otra vulnerabilidad de día cero que ha resuelto Microsoft (CVE-2023-29325) se encuentra en el software Microsoft Outlook. Es un fallo de OLE que puede ser explotado mediante el uso de correos electrónicos especialmente diseñados.

Microsoft también ha abordado otras vulnerabilidades con puntuaciones CVSS notablemente altas en su actualización de Patch Tuesday de mayo de 2023.