Vulnerabilidades de sistemas

Seguridad Informática

Juan Carlos Navidad García

Todas las vulnerabilidades son sacadas de Incibe.es

Últimas vulnerabilidades de Windows:

- **Print Spooler:** Se ha detectado una vulnerabilidad severidad alta que afecta al servicio de cola de impresión de Windows que podría permitir a un ciberatacante realizar una ejecución remota de código.
- **Elevación de privilegios:** Ha sido reportada a Microsoft una vulnerabilidad de severidad alta que afecta a varias versiones de Windows. Esta vulnerabilidad podría permitir a un ciberatacante realizar una ejecución de código o la creación, modificación o eliminación de archivos por un error de privilegios.
- **0-Day Internet Explorer:** Microsoft ha publicado un boletín de seguridad avisando sobre una vulnerabilidad que afecta al navegador Internet Explorer. Un ciberdelincuente, utilizando un sitio web especialmente diseñado, podría explotar la vulnerabilidad para realizar acciones maliciosas que afecten a la privacidad y seguridad de la empresa.

Últimas vulnerabilidades de Linux:

- **Vulnerabilidad Bluetooth:** Ingenieros de Google han informado de la existencia de varias vulnerabilidades que afectan a la pila que se encarga de gestionar el envío y la recepción de paquetes en las conexiones Bluetooth.
  Dichas vulnerabilidades permitirían a un ciberatacante realizar una escalada de privilegios, permitiéndole realizar otras acciones malintencionadas en el dispositivo afectado, tales como la ejecución de código malicioso, el robo de información o el ataque de denegación de servicio contra el dispositivo.

- **Vulnerabilidad en las suites de ofimática OpenOffice y LibreOffice:** Se ha descubierto una vulnerabilidad que afecta a los paquetes ofimáticos LibreOffice y OpenOffice que podría permitir a un atacante ejecutar código remoto o acceder a información confidencial de la víctima.

- **Fallo de software en un componente de Linux muy utilizado en dispositivos y software**: El equipo de investigadores de Google y Red Hat han descubierto una vulnerabilidad en un componente (la librería glibc) software utilizado en muchas aplicaciones y dispositivos basados en el sistema operativo Linux (entre ellos routers, servidores, etc.) que podría afectar seriamente cuando se conectan a Internet utilizando este componente.
  Dicho componente se utiliza para hacer peticiones a los servidores DNS (donde se traducen las peticiones de páginas web a las direcciones que entiende Internet).
  Los posibles ataques que aprovechen esta vulnerabilidad pueden tomar un control completo de los dispositivos y aplicaciones que lo utilicen.

Últimas vulnerabilidades de Internet Explorer:

- **0-Day Internet Explorer:** Microsoft ha publicado un boletín de seguridad avisando sobre una vulnerabilidad que afecta al navegador Internet Explorer. Un ciberdelincuente, utilizando un sitio web especialmente diseñado, podría explotar la vulnerabilidad para realizar acciones maliciosas que afecten a la privacidad y seguridad de la empresa.

- **Ejecución remota de código en Internet Explorer:** Microsoft está investigando una vulnerabilidad de severidad alta que afecta a varias versiones de Windows a través de un componente de Internet Explorer, MSHTML, que se utiliza para mostrar documentos. Esta vulnerabilidad, que está siendo explotada utilizando documentos de Microsoft Office especialmente diseñados, podría permitir a un ciberatacante realizar una ejecución remota de código en el sistema vulnerable.

- **Vulnerabilidades en Microsoft Internet Explorer y Microsoft Defender:** Microsoft ha corregido dos vulnerabilidades fuera de su ciclo de actualizaciones, mediante las cuales un ciberdelincuente podría ejecutar código malicioso remotamente y de esta manera hacerse con el control del equipo o generar una condición de denegación de servicio.

Últimas vulnerabilidades de Mozilla Firefox:

- **Vulnerabilidad en un archivo que carece de una extensión en Windows en el panel de descargas en Firefox, Thunderbird y Firefox ESR (CVE-2020-35112):** Si un usuario descargó un archivo que carece de una extensión en Windows y luego "Open"-ed desde el panel de descargas, si había un archivo ejecutable en el directorio de descargas con el mismo nombre pero con una extensión ejecutable (como .bat o .exe) ese ejecutable habría sido iniciado en su lugar. *Nota: este problema solo afectó a unos sistemas operativos Windows. Otros sistemas operativos no están afectados.*. Esta vulnerabilidad afecta a Firefox versiones anteriores a 84, Thunderbird versiones anteriores a 78,6 y Firefox ESR versiones anteriores a 78,6.

- **Vulnerabilidad en el análisis y la carga de eventos en el código SVG de Firefox en Firefox, Firefox ESR y Thunderbird (CVE-2020-26951):** Un desajuste en el análisis y la carga de eventos en el código SVG de Firefox podría haber permitido a unos eventos de carga dispararse, incluso después del saneamiento. Un atacante ya capaz de explotar una vulnerabilidad de tipo XSS en páginas internas privilegiadas podría haber usado este ataque para omitir nuestro sanitizador incorporado. Esta vulnerabilidad afecta a Firefox versiones anteriores a 83, Firefox ESR versiones anteriores a 78.5, y Thunderbird versiones anteriores a 78.5.

- **Vulnerabilidad crítica:** La vulnerabilidad catalogada como crítica podría permitir, en determinadas circunstancias, mediante las operaciones realizadas con datos de tipo BigInt (dato numérico), obtener la información almacenada en memoria y que no ha sido utilizada, lo que se traduce en la posibilidad de que un ciberdelincuente pueda leer dicha información y usarla para realizar otras actividades maliciosas.