Práctica – Vulnerabilidades

1. Hispasec (http://www.hispasec.com/ - sección “una-al-día”)
    - Funcionalidad: Publica diariamente noticias breves sobre vulnerabilidades, incidentes de seguridad, malware y amenazas actuales.
    - Responsable: Hispasec Sistemas, empresa española dedicada a la consultoría y servicios de ciberseguridad.
2. NVD (http://nvd.nist.gov/ - National Vulnerability Database)
    - Funcionalidad: Base de datos oficial de vulnerabilidades gestionada por el gobierno de EE. UU. Contiene información técnica sobre CVEs, puntuaciones CVSS, métricas de impacto y soluciones recomendadas.
    - Responsable: NIST, un organismo del Departamento de Comercio de EE. UU.
3. INCIBE (http://www.incibe.es - buscador de vulnerabilidades)
    - Funcionalidad: El Instituto Nacional de Ciberseguridad de España ofrece un portal con avisos de seguridad, buscador de vulnerabilidades, alertas técnicas y recursos formativos.
    - Responsable: INCIBE, entidad pública dependiente del Ministerio de Asuntos Económicos y Transformación Digital del Gobierno de España.

Web propuesta:

- Exploit Database (https://www.exploit-db.com/)

  Permite a un desarrollador conocer no solo la vulnerabilidad, sino también la forma práctica en que un atacante podría aprovecharla, mejorando la capacidad de prevenir errores similares en sus propios proyectos.

Noticia elegida: *HybridPetya: el nuevo ransomware que combina técnicas de Petya y WannaCry* (publicada en Hispasec "una-al-día").

Resumen:
HybridPetya es un ransomware que se propagó de forma masiva en 2017 afectando a empresas e instituciones en varios países. Se caracterizó por combinar técnicas de Petya (que cifra la tabla MFT del disco, impidiendo el arranque) con las capacidades de propagación de WannaCry mediante EternalBlue, una vulnerabilidad en SMB de Windows. Además, se descubrió que su objetivo real parecía más destructivo que económico, ya que el mecanismo de recuperación de archivos era ineficaz.

Elegí esta noticia porque demuestra cómo los atacantes combinan vulnerabilidades ya conocidas para crear amenazas más potentes y difíciles de contener. Además, ilustra la importancia de aplicar parches de seguridad de forma constante, ya que EternalBlue ya contaba con solución antes de la campaña. Su impacto global y mediático lo convierte en un ejemplo clave de vulnerabilidad crítica en sistemas empresariales.

Bug localizado:

- CVE: CVE-2023-21716
- Programa afectado: Microsoft Word
- Versión: Afecta a versiones de Microsoft Office 2013, 2016, 2019 y Microsoft 365 (previo a los parches de febrero 2023).
- Nivel de gravedad: Crítico (CVSS 9.8).
- Descripción:
  Se trata de una vulnerabilidad de ejecución remota de código (RCE). Un atacante puede explotar el fallo a través de un documento de Word especialmente diseñado. Basta con que la víctima abra el archivo malicioso para que el atacante ejecute código arbitrario en el sistema con los privilegios del usuario afectado.
  El fallo se debe a un manejo incorrecto de la conversión RTF en Word. Microsoft lo corrigió en su "Patch Tuesday" de febrero 2023.

Proyecto OWASP y OWASP Top Ten:

- OWASP (Open Web Application Security Project):
  Es una comunidad internacional sin ánimo de lucro enfocada en mejorar la seguridad del software. Su misión es proporcionar documentación, herramientas y estándares abiertos que permitan a desarrolladores y organizaciones crear aplicaciones seguras. OWASP se organiza en capítulos locales, proyectos comunitarios, conferencias y publicaciones.
- OWASP Top Ten:
  Es uno de los proyectos más influyentes de OWASP. Consiste en un listado que se publica cada pocos años con las 10 vulnerabilidades más críticas en aplicaciones web, basado en datos recopilados de la industria y análisis de expertos. Su objetivo es concienciar y ofrecer una guía práctica para que los desarrolladores prioricen medidas de seguridad.
  Ejemplos de vulnerabilidades incluidas: inyección SQL, fallos de autenticación, exposición de datos sensibles, deserialización insegura, entre otras.
  Su utilidad radica en que se ha convertido en un estándar de facto para auditar, desarrollar y formar en seguridad de aplicaciones.