PRESNTACION A9: 2017: uso de componentes con vulnerabilidades conocidas

Miguel Romero Suarez

OWASP

OWASP es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro. La Fundación OWASP es un organismo sin ánimo de lucro que apoya y gestiona los proyectos e infraestructura de OWASP

A9: 2017: uso de componentes con vulnerabilidades conocidas

- Si bien es fácil encontrar exploits ya escritos para muchas vulnerabilidades conocidas, otras vulnerabilidades requieren un esfuerzo concentrado para desarrollar un exploit personalizado.
  Los componentes, como bibliotecas, marcos y otros módulos de software, se ejecutan con el mismo privilegios como la aplicación. Si se explota un componente vulnerable, dicho ataque puede facilitar pérdida grave de datos o adquisición del servidor. Aplicaciones y API que usan componentes con conocidos Las vulnerabilidades pueden debilitar las defensas de las aplicaciones y permitir varios ataques e impactos.

Debilidad de seguridad

- La prevalencia de este problema está muy extendida. Los patrones de desarrollo con muchos componentes pueden hacer que los equipos de desarrollo ni siquiera comprendan qué componentes usan en su aplicación o API, y mucho menos mantenerlos actualizados. Algunos escáneres como retire.js ayudan en la detección, pero determinar la explotabilidad requiere un esfuerzo adicional.

Impactos

- Si bien algunas vulnerabilidades conocidas provocan solo impactos menores, algunas de las violaciones más grandes hasta la fecha se han basado en la explotación de vulnerabilidades conocidas en los componentes. Dependiendo de los activos que esté protegiendo, tal vez este riesgo debería estar en la parte superior de la lista.

¿Es la aplicación vulnerable?

- Si no conoce las versiones de todos los componentes que usa. Esto incluye componentes que usa directamente, así como dependencias anidadas.
- Si el software es vulnerable, no es compatible o está desactualizado. Esto incluye el sistema operativo, el servidor web / de aplicaciones, el sistema de administración de bases de datos (DBMS), las aplicaciones, las API y todos los componentes, entornos de tiempo de ejecución y bibliotecas.
- Si no explora las vulnerabilidades regularmente y se suscribe a los boletines de seguridad relacionados con los componentes que utiliza.
- Si no arregla ni actualiza la plataforma, los marcos y las dependencias subyacentes de manera oportuna y basada en el riesgo. Esto ocurre comúnmente en entornos en los que la aplicación de parches es una tarea mensual o trimestral bajo control de cambios, lo que deja a las organizaciones abiertas a muchos días o meses de exposición innecesaria a vulnerabilidades fijas.
- Si los desarrolladores de software no prueban la compatibilidad de las bibliotecas actualizadas, actualizadas o parcheadas.
- Si no protege las configuraciones de los componentes en la cual tiene que ver la vulnerabilidad **A6: 2017 - Configuración incorrecta de seguridad** .

Como prevenir

Debe haber un proceso de administración de parches para:

- Elimine dependencias no utilizadas, características innecesarias, componentes, archivos y documentación.
- Haga un inventario continuo de las versiones de los componentes del lado del cliente y del lado del servidor
- Solo obtenga componentes de fuentes oficiales a través de enlaces seguros
- Supervise las bibliotecas y los componentes que no están mantenidos o que no crean parches de seguridad para versiones anteriores

Es importante saber que

- Existen herramientas automatizadas para ayudar a los atacantes a encontrar sistemas sin parches o mal configurados. Por ejemplo, el motor de búsqueda Shodan IoT puede ayudarlo a encontrar dispositivos que aún sufren de la vulnerabilidad Heartbleed que fue parcheada en abril de 2014.