Ataque de día cero

Describe vulnerabilidades de seguridad recién descubiertas que los hackers usan para atacar un sistema. Se refiere al hecho de que el proveedor o desarrollador acaba de conocer una falla, lo que significa que ha tenido “cero días” para corregirla. Es muy importante entender la diferencia entre vulnerabilidad, exploit, ataque.

- Vulnerabilidad: Es la puerta de entra que utiliza un ciberdelincuente para afectar un sistema en específico, ya que los desarrolladores no conocen de su existencia no existen parches de seguridad.
- Exploit: Es el método de ataque que utilizan los ciberdelincuentes para atacar un sistema con la vulnerabilidad no parcheada.
- Ataque: Es el uso del exploit de día cero para causar daños o robot datos a un sistema infectado.

Ejemplos

Vulnerabilidad de Chrome

En 2021, Google Chrome sufrió una serie de amenazas de este estilo, lo cual causo que Chrome lanzará actualizaciones para esta vulnerabilidad, la cual se debía a un error en el motor de búsqueda V8 JavaScript que utiliza este navegador.

iOS de Apple

En el 2020, fue víctima de al menos dos conjuntos de vulnerabilidades de día cero de iOS, las que incluían un error de día cero que permitía a los atacantes comprometer los iPhone de forma remota.

Zoom

En 2020, se encontró una vulnerabilidad en esta plataforma; la cual permitía a los ciberdelincuentes acceder de forma remota a la computadora de un usuario que utilizara una versión de Windows antigua.