CIBERCONSEJOS

VULNERABILIDADES

CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

¿Qué es una vulnerabilidad?

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

En el mundo de la tecnología, llamamos vulnerabilidad a errores de diseño de los programas de software que funcionan como un punto débil, facilitando el accionar de ciberdelincuentes.

Así, una vulnerabilidad puede permitir a un actor malicioso ingresar sin autorización a nuestra información e incluso tomar control de nuestros equipos.

Algunos riesgos a los que nos exponen:

- Instalación de programas maliciosos (malware).
- Acceso no autorizado y modificación de datos.
- Destrucción o alteración de datos de un sistema.
- Daño a dispositivos con conexión a internet.

Cuando se descubre una vulnerabilidad nueva, se les conoce como de día cero, o zero day.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Las actualizaciones de software parchan las nuevas vulnerabilidades

Las empresas de software publican actualizaciones de sus productos cuando descubren nuevas vulnerabilidades.

Estas actualizaciones de seguridad resuelven estas vulnerabilidades, para que dejen de ser un problema. En ciberseguridad, a estas correcciones se les llama comúnmente “parches”.

Por todo esto, es muy importante actualizar nuestros programas, incluyendo sistemas operativos y apps, tan pronto como sea posible.

Lo idea es activar las actualizaciones de seguridad automáticas.

Y como siempre, descargar programas y actualizaciones únicamente de sitios oficiales

Algunos tipos de vulnerabilidades, según lo que permiten al malhechor:

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

- Ejecución remota de código (RCE): Permite ejecutar código en el sistema vulnerable, sin autorización.
- Inyección de SQL: Posibilita a un atacante ejecutar comandos SQL no autorizados a través de una entrada no controlada.
- Cross site scripting (XSS): Usado para afectar páginas web a través de la inyección de scripts maliciosos.
- Desbordamiento de buffer: Se envían maliciosamente más datos de los que el software vulnerable puede manejar, permitiendo al atacante sobrescribir la memoria adyacente.
- Denegación de servicio (DoS): Facilita que el atacante deje sin disponibilidad un sitio o servicio web.