	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 071	Fecha: 23-03-2023
		Página 5 de 25

Componente que reporta	**COMANDO OPERACIONAL DE CIBERDEFENSA DEL COMANDO CONJUNTO DE LAS FUERZAS ARMADAS**		
Nombre de la alerta	Hackers informáticos armaron y explotaron más de 55 días cero en Microsoft, Google y Apple		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de subfamilia	C02
Clasificación temática familia	Código malicioso		

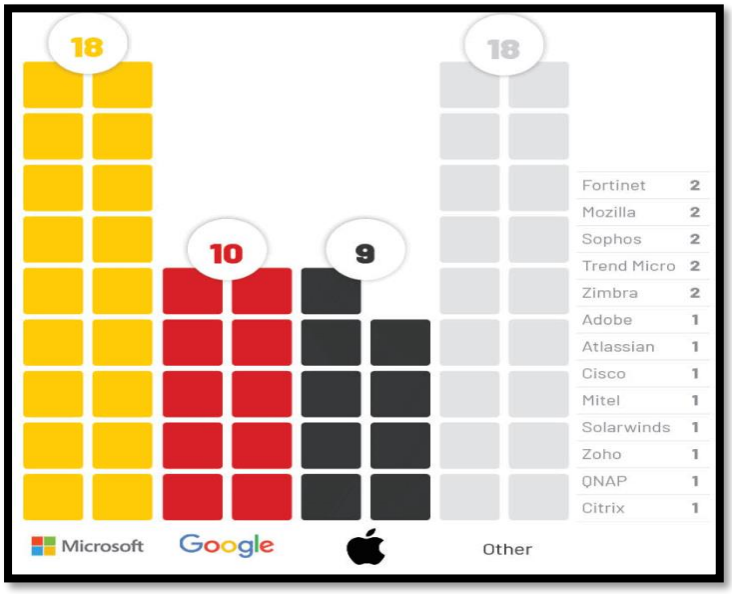
Descripción

1. Se tuvo conocimiento que hackers informáticos armaron y explotaron más de 55 días cero en Microsoft, Google y Apple. Los investigadores afirman que los hackers informáticos siguen apuntando a las vulnerabilidades de día cero en campañas maliciosas, también se informó que la mayoría de estas vulnerabilidades dieron como resultado que el atacante pudiera obtener privilegios elevados o ejecutar código remoto en dispositivos vulnerables.

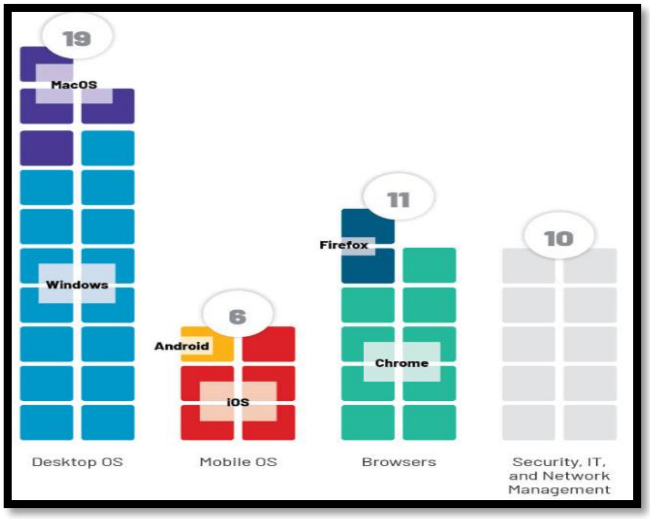
   Una vulnerabilidad de día cero es un riesgo de seguridad del software que el proveedor o el usuario del software desconocen, donde ataques son una amenaza para la seguridad de los sistemas informáticos y las redes ya que aprovechan vulnerabilidades previamente desconocidas que aún no se han detectado o reparado.

   En el año 2022 hubo 55 fallas de día cero explotadas; 13 fueron explotados por grupos de ciberespionaje, mientras que los ciberespías chinos explotaron 7, lo que convierte al país en el más productivo.

   El informe de la empresa Mandiant de Ciberseguridad encontró que los tres proveedores de tecnología más grandes del mundo, Microsoft, Google y Apple, fueron los proveedores más comúnmente explotados por tercer año consecutivo, con 18, 10 y 9 vulnerabilidades de día cero, respectivamente.



   Los tipos de productos afectados con mayor frecuencia fueron los sistemas operativos (19), los navegadores (11), los productos de seguridad, TI y administración de redes (10) y los sistemas operativos móviles (6). El informe reveló que los sistemas operativos de escritorio fueron los más explotados, con 19 vulnerabilidades de día cero identificadas; Windows fue el más afectado, con 15 fallas, seguido de macOS con 4, en el caso de los sistemas operativos móviles, se explotaron 5 fallas en iOS y 1 en Android.



2. RECOMENDACIONES:

- Las organizaciones implementen medidas de seguridad firewalls y sistemas de detección de intrusos.
- Mantener el software y los sistemas de seguridad actualizados.
- En lugar de exponer sus servidores a Internet, use túneles privados o VPN para acceder a ellos.
- Asegúrese de instalar cortafuegos.
- Garantizar el uso de productos de filtrado web y de correo electrónico.

Fuentes de información	▪ hxxps://gbhackers.com/ ▪ hxxps://altadensidad.com