A continuación, te proporciono una breve descripción de cada uno de los CVEs mencionados, incluyendo las tecnologías o fabricantes afectados y algunos de los ataques conocidos que han tenido repercusión en los medios:

1. CVE-2019-0708:

- Tecnologías/Fabricantes Afectados: Este CVE afecta a los sistemas operativos Microsoft Windows, específicamente a las versiones Windows 7 y Windows Server 2008, que utilizan el Protocolo de Escritorio Remoto (RDP).

- Descripción: CVE-2019-0708, comúnmente conocido como "BlueKeep," es una vulnerabilidad crítica en el servicio RDP de Windows. Permite la ejecución remota de código sin necesidad de autenticación, lo que significa que un atacante podría tomar el control total de un sistema vulnerable sin necesidad de credenciales.

- Ataques Conocidos: Aunque no se informaron ataques generalizados, la preocupación sobre la gravedad de esta vulnerabilidad llevó a Microsoft a emitir parches y advertencias para su corrección.

2. CVE-2020-10148:

- Tecnologías/Fabricantes Afectados: Este CVE se relaciona con el software de virtualización VMware vCenter Server.

- Descripción: CVE-2020-10148 es una vulnerabilidad crítica que afecta al software de administración de centros de datos VMware vCenter Server. La vulnerabilidad permite a un atacante remoto ejecutar comandos en el sistema afectado sin autenticación.

- Ataques Conocidos: La vulnerabilidad se dio a conocer en junio de 2020, y VMware emitió rápidamente parches para solucionarla. Hasta donde se sabe, no se informaron ataques generalizados antes de que se aplicaran los parches.

3. CVE-2022-23307:

- Tecnologías/Fabricantes Afectados: Este CVE se encuentra en el software de firewall de código abierto pfSense, utilizado para la protección de redes.

- Descripción: CVE-2022-23307 es una vulnerabilidad que afecta al sistema de filtrado de paquetes pfSense, un firewall basado en FreeBSD. Esta vulnerabilidad podría permitir a un atacante remoto eludir las reglas de firewall o causar una denegación de servicio.

- Ataques Conocidos: Los detalles específicos sobre los ataques conocidos no están disponibles en mi base de datos, ya que la vulnerabilidad es relativamente reciente (2022). Sin embargo, se recomienda a los usuarios de pfSense que apliquen las actualizaciones de seguridad proporcionadas por los desarrolladores para mitigar este riesgo.

Es importante destacar que la información sobre vulnerabilidades y ataques puede cambiar con el tiempo, por lo que es fundamental mantenerse actualizado mediante fuentes de seguridad confiables y aplicar parches o soluciones cuando estén disponibles para proteger tus sistemas y redes.