Índice:

Ejercicio 5

a) Realiza un breve informe sobre vulnerabilidades actuales detectas en aplicaciones y sistemas operativos como Windows, Linux, Apple, Android, Chrome

Solución:

Windows 13 Septiembre 2023

CVE-2023-38148: Vulnerabilidad de ejecución remota de código de Internet Connection Sharing (ICS).

CVE-2023-29332: Vulnerabilidad de elevación de privilegios en el servicio Kubernetes de Microsoft Azure.

CVE-2023-36793 / CVE-2023-36792 / CVE-2023-36796: Vulnerabilidad de ejecución remota de código en Visual Studio.

Linux 6 Julio 2023

StackRot (CVE-2023-3269) fue descubierta e informada por el investigador de seguridad Ruihan Li. Según Li, esta vulnerabilidad afecta al subsistema de administración de memoria del kernel de Linux, que es responsable de implementar la memoria virtual, la paginación de demanda y la asignación de memoria para los programas del kernel y del espacio de usuario.

Apple 8 Septiembre 2023

CVE-2023-41064, permitía que dispositivos como iPhone y iPad fueran vulnerables al procesar una imagen creada con fines malintencionados y afectaba al framework Image I/O. La otra vulnerabilidad, CVE-2023-41061, fue descubierta por la propia Apple y actuaba de forma similar, pero en su caso surgió en el Wallet y activaba la exploit chain cuando el dispositivo recibía archivo adjunto creado con fines malintencionados.

Android 6 de Septiembre

3 de ejecución remota de código que afectan a system (CVE-2023-35658, CVE-2023-35673 y CVE-2023-35681) que podrían permitir a un atacante realizar una escalada de privilegios, divulgar información y provocar una denegación de servicio (DoS) o hacer una ejecución de código remota (RCE)

Chrome 12 Septiembre

Google insta a actualizar Chrome para corregir una vulnerabilidad crítica de día cero activamente explotada Google ha lanzado un parche de seguridad para el navegador Chrome con el que corrige una vulnerabilidad crítica que pone en riesgo el equipo, ya que provoca desde fallo de sistema hasta la ejecución de código arbitrario.