TLP: CLEAR : Se usa cuando la información no genera ningún riesgo de mal uso y pueda ser difundido de forma pública. En este sentido, la información puede ser distribuida sin restricciones, pero sujeta a controles de derechos de autor

Julio 2 de 2024

INFORME DE VULNERABILDIAD EN SERVICIO OpenSSH

La empresa Qualys[1] ha identificado una vulnerabilidad crítica de ejecución de código remoto en OpenSSH, conocida como "RegreSSHion"[2]. Esta vulnerabilidad afecta las versiones desde 8.5p1 hasta 9.8p1, así como la versión original 4.4p1. La causa principal de esta vulnerabilidad es la eliminación de un parche de seguridad implementado en 2006, lo que permite a los atacantes ejecutar código con privilegios de super usuario.

Detalles de la Vulnerabilidad:

- CVE-2024-6387[3]
- CVE-2006-5051[4]
- Impacto: Ejecución de código remoto con privilegios de super usuario.
- Versiones afectadas: OpenSSH 8.5p1 a 9.8p1 y 4.4p1.
- Exclusiones: Sistemas basados en OpenBSD.

Recomendaciones de remediación:

- Actualizar OpenSSH a 9.8p1 o superior

Otras recomendaciones

- Configurar reglas de firewall para restringir el acceso SSH solo a direcciones IP de confianza.
- Implementar segmentación de redes para limitar el alcance de un posible ataque.

Cordialmente

CSIRT Académico UNAD
Correo electrónico: csirt@unad.edu.co
(+57 1) 344 37 00 Ext. 1042516

[1] https://www.qualys.com/
[2] https://blog.qualys.com/vulnerabilities-threat-research/2024/07/01/regresshion-remote-unauthenticated-code-execution-vulnerability-in-openssh-server
[3] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-6387
[4] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5051