`vulnerability-report`

Según la información otorgada después de un NMAP se reporta que los Servidores de Apache2 y OpenSSH cuentan con las siguientes vulnerabilidades

OpenSSH 9.9p1 Denial of Service / Man-In-The-Middle Vulnerability

OpenSSH tiene vulnerabilidades que permiten ataques Man-In-The-Middle y Denegación de servicio.

Las versiones de OpenSSH 6.8p1 a 9.9p1 contienen un error lógico que permite a un atacante en la ruta (también conocido como intermediario) hacerse pasar por cualquier servidor cuando la opción VerifyHostKeyDNS está habilitada. Esta opción está desactivada de forma predeterminada. Las versiones de OpenSSH 9.5p1 a 9.9p1 son vulnerables a una denegación de servicio de memoria/CPU relacionada con el manejo de paquetes SSH2_MSG_PING. Esta condición se puede mitigar utilizando la función PerSourcePenalties existente.

en el caso de OpenSSH 9.2p1 y:

Apache httpd -- Multiple vulnerabilities

Fundación de software Apache
SSRF en el servidor Apache HTTP en Windows con mod_rewrite en el contexto de servidor/vhost, permite potencialmente filtrar hashes NTML a un servidor malicioso a través de SSRF y solicitudes maliciosas. Se recomienda a los usuarios actualizar a la versión 2.4.65, que soluciona este problema.

Recomendaciones

Se recomienda actualizar a versiones mas recientes como Apache2 Httpd 2.4.65 y OpenSSH 10 las cuales no cuentan con las ya advertidas vulnerabilidades.