OpenBSD, un sistema operativo de código abierto, creado con la seguridad como principal objetivo, se ha encontrado vulnerable a cuatro nuevas vulnerabilidad graves, una de las cuales es una vulnerabilidad de omisión de autenticación de tipo antiguo en el marco de BSD Auth.

Las tres vulnerabilidades restantes son problemas de escalada de privilegios que podrían permitir a los usuarios locales o software malintencionado, obtener privilegios de un grupo de autenticación, root, así como de otros usuarios respectivamente.

Las vulnerabilidades fueron descubiertas e informadas por Qualys Research Labs, a inicios de esta semana. En respuesta a esto, los desarrolladores de OpenBSD lanzaron parches de seguridad para OpenBSD 6.5 y OpenBSD 6.6 ayer.

OpenSDB es un sistema operativo tipo Unix basado en BSD gratuito y de código abierto, a continuación se detallan las vulnerabilidades encontradas.

Bypass de autenticación de OpenBSD (CVE-2019-19521)

La vulnerabilidad de omisión de autenticación reside en la forma en que el marco de autenticación de OpenBSD analiza el nombre de usuario proporcionado por un usuario al iniciar sesión por medio de los servicios smtpd, ldapd, radiusd, su o sshd.

Al utilizar esta falla, un atacante remoto puede acceder con éxito a servicios vulnerables con cualquier contraseña simplemente ingresando el nombre de usuario como «-schallenge» o «-schallenge:passwd», y funciona porque un guión antes del nombre de usuario engaña a OpenBSD para que interprete el valor como una opción de línea de comandos y no como un nombre de usuario.

El marco de autenticación de OpenBSD interpreta «-schallenge» como «-s challenge», lo que

obliga al sistema a ignorar silenciosamente el protocolo de desafío que eventualmente omite la autenticación de forma automática.

> *«Si un atacante especifica un nombre de usuario con el formulario '-option', puede influir en el comportamiento del programa de autenticación de formas inesperadas»,* dice el aviso.

Según los investigadores, esta vulnerabilidad es prácticamente explotable en smtpd, ldapd y radiusd, pero no en sshd debido a sus mecanismos de defensa en profundidad que bloquean la conexión incluso después de una omisión de autenticación exitosa.

Sin embargo, todavía se puede explotar remotamente la falla contra sshd para determinar si un sistema OpenBSD es vulnerable a CVE-2019-19521 o no.

Defectos de escalada de privilegios locales de OpenBSD

- CVE-2019-19520: Debido al mal manejo de las rutas proporcionadas por el entorno utilizadas en dlopen (), xlock, que viene instalado por defecto en OpenBSD, podría permitir a los atacantes locales escalar privilegios al grupo 'auth'.
- CVE-2019-19522: Debido al funcionamiento incorrecto de los mecanismos de autorización a través de «S /Key» y «YubiKey», que es una configuración no predeterminada, un atacante local con permiso de grupo 'auth' puede obtener todos los privilegios del usuario root.
- CVE-2019-19519: Debido a un error lógico en una de las funciones principales, un atacante local puede lograr la clase de inicio de sesión de cualquier usuario, a menudo excluyendo root, explotando la opción -L de SU.

Los investigadoresde Qualys también lanzaron exploits de prueba de concepto para cada vulnerabilidad en su aviso.

Debido a que los parches para las cuatro vulnerabilidades de seguridad ahora están disponibles, los usuarios de OpenBSD afectados recomendaron instalar parches utilizando el mecanismo syspatch.