Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

NUEVA VULNERABILIDAD CRÍTICA EN OPENSSH PERMITE EJECUCIÓN REMOTA DE CÓDIGO EN SERVIDORES LINUX

03 / 07 / 2024

CONTENIDO

INTRODUCCIÓN

Recientemente, se ha descubierto una vulnerabilidad crítica en OpenSSH denominada "regreSSHion", que permite la ejecución remota de código (RCE) y concede privilegios de root en sistemas Linux basados en glibc. Identificada como CVE-2024-6387 y descubierta por investigadores de Qualys, esta falla de seguridad podría llevar a la toma de control completa de los servidores afectados, subrayando la importancia de una rápida respuesta y la implementación de medidas de mitigación adecuadas para proteger la infraestructura tecnológica de las organizaciones.

NUEVA VULNERABILIDAD CRÍTICA EN OPENSSH PERMITE EJECUCIÓN REMOTA DE CÓDIGO EN SERVIDORES LINUX

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2024_07_03_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	03/07/2024
Es día cero (0 day):	No

RESUMEN

En el ámbito de la ciberseguridad, se ha descubierto una nueva vulnerabilidad crítica en OpenSSH que afecta a servidores Linux basados en glibc. Denominada “regreSSHion”, esta vulnerabilidad permite a atacantes remotos ejecutar código arbitrario con privilegios de root, comprometiendo severamente la seguridad de los sistemas afectados.

Detalles De La Vulnerabilidad

La vulnerabilidad CVE-2024-6387 fue identificada por investigadores de Qualys en mayo de 2024. Se trata de una condición de carrera en el manejador de señales de SSHD, donde un atacante no autenticado puede aprovechar un error en el manejo de señales para ejecutar código malicioso con los más altos privilegios del sistema.

Según un boletín de seguridad de Debian, “si un cliente no se autentica dentro del tiempo de LoginGraceTime (por defecto, 120 segundos), el manejador SIGALRM de SSHD es llamado de manera asincrónica y ejecuta varias funciones que no son seguras para señales asíncronas”.

Impacto Y Consecuencias

La explotación de regreSSHion podría resultar en la toma completa del sistema, permitiendo a los atacantes instalar malware, manipular datos, y crear backdoors para un acceso persistente. Esto podría facilitar la propagación en la red, comprometiendo otros sistemas vulnerables dentro de la organización.

Qualys señala que, a pesar de la severidad de la vulnerabilidad, explotar regreSSHion puede ser complejo y requiere múltiples intentos para lograr la corrupción de memoria necesaria. No obstante, advierten que herramientas de inteligencia artificial podrían facilitar la explotación exitosa.

> “This vulnerability, if exploited, could lead to full system compromise where an attacker can execute arbitrary code with the highest privileges, resulting in a complete system takeover, installation of malware, data manipulation, and the creation of backdoors for persistent access. It could facilitate network propagation, allowing attackers to use a compromised system as a foothold to traverse and exploit other vulnerable systems within the organization.”
>
> ❖ Qualys

Medidas De Mitigación

Para mitigar el riesgo de regreSSHion, se recomienda tomar las siguientes acciones:

•Aplicar la última actualización disponible para el servidor OpenSSH (versión 9.8p1), que corrige esta vulnerabilidad.

•Restringir el acceso SSH utilizando controles basados en red como firewalls, e implementar segmentación de red para prevenir movimientos laterales.

•En caso de no poder actualizar inmediatamente, ajustar el 'LoginGraceTime' a 0 en el archivo de configuración de SSHD, aunque esto puede exponer al servidor a ataques de denegación de servicio.

Conclusiones

A pesar de que OpenBSD no se ve afectado gracias a un mecanismo seguro introducido en 2001, se recomienda realizar análisis separados para determinar la vulnerabilidad en macOS y Windows. La comunidad de seguridad recomienda una respuesta rápida y efectiva para proteger los sistemas críticos de las organizaciones.

Este tipo de vulnerabilidades subraya la importancia de mantener los sistemas actualizados y contar con prácticas robustas de ciberseguridad para proteger la integridad de los datos y la continuidad del negocio.

NOTICIA COMPLETA

https://devel.group/blog/nueva-vulnerabilidad-critica-en-openssh-permite-ejecucion-remota-de-codigo-en-servidores-linux/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente