Boletín de alerta

Boletín Nro.:
Fecha de publicación: 23/06/2026
Tema: Alerta 2026-67 Vulnerabilidad Crítica de Ejecución Remota de Código en libssh2
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

Versiones afectadas:

- **libssh2 ≤ 1.11.1**

Distribuciones identificadas como vulnerables:

- **Debian 11 (Bullseye) – 1.9.0-2+deb11u1**
- **Debian 12 (Bookworm) – 1.10.0-3**
- **Debian Testing (Trixie) – 1.11.1-1**
- **Debian Sid/Forky – 1.11.1-3**

Descripción

Se ha reportado una vulnerabilidad crítica que afecta a libssh2, la misma fue etiquetada como CVE-2026-55200 con un CVSS 9.2. La biblioteca libssh2 es ampliamente utilizada para establecer conexiones SSH seguras.

La falla se origina en la función ssh2_transport_read(), la cual no valida correctamente el tamaño del campo packet_length dentro de los paquetes SSH recibidos.

Un servidor SSH malicioso, comprometido o controlado por un atacante mediante una técnica de Man-in-the-Middle (MITM) puede enviar paquetes especialmente manipulados con tamaños excesivos, provocando una corrupción de memoria tipo Out-of-Bounds Write.

La explotación exitosa puede permitir la ejecución remota de código en el sistema cliente que establece la conexión SSH, otorgando al atacante la capacidad de ejecutar comandos arbitrarios, instalar malware, robar información o comprometer completamente el equipo afectado.

Solución:

Actualizar libssh2 a una versión que incluya el parche publicado en el commit.

transport.c: Additional boundary checks for packet length (#2052) · libssh2/libssh2@97acf3d · GitHub

Oficialmente aún no se ha publicado un parche con la solución. Es importante de estar pendientes de novedades al respecto.

Información adicional:

- CVE-2026-55200
- CVE-2026-55200 | Ubuntu
- NVD – CVE-2026-55200
- libssh2: security issues CVE-2026-55199 and CVE-2026-55200 · Issue #532920 · NixOS/nixpkgs
- transport.c: Additional boundary checks for packet length (#2052) · libssh2/libssh2@97acf3d · GitHub