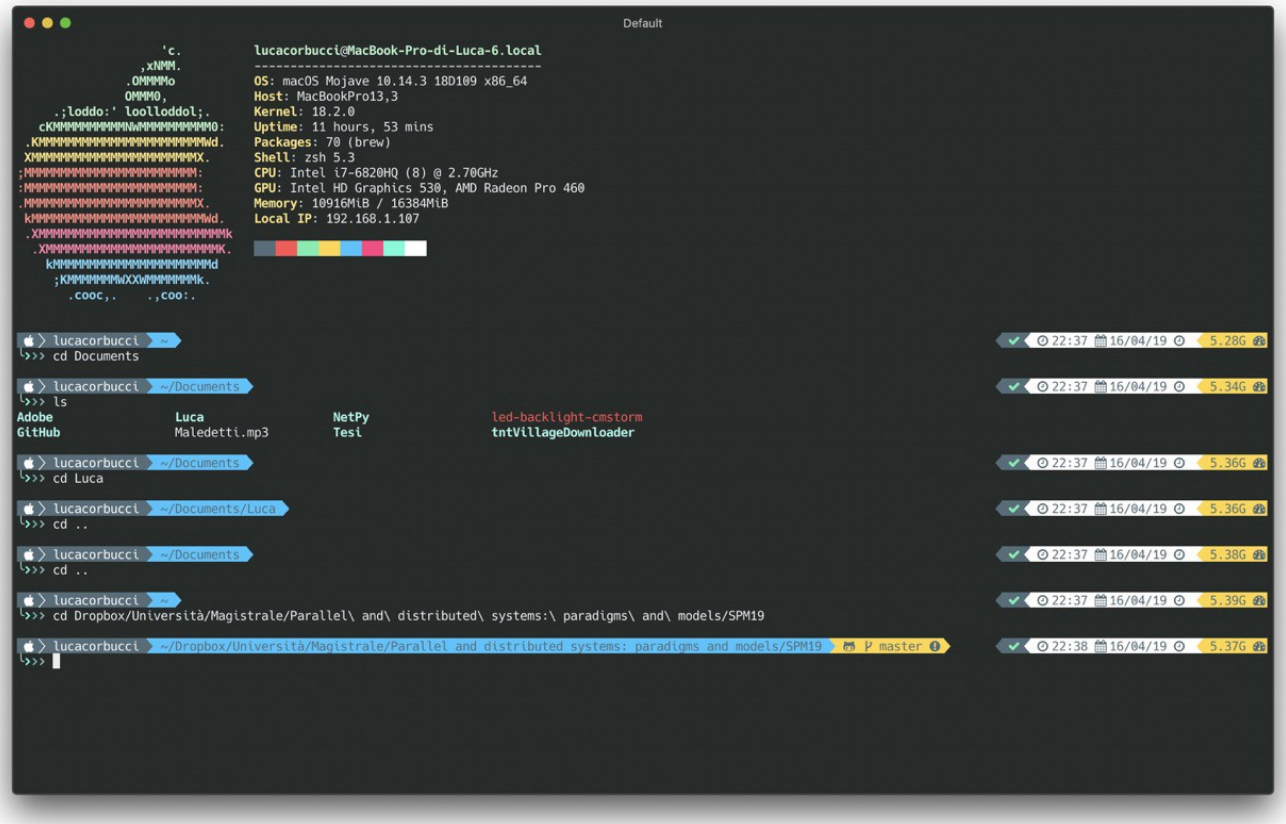
Vulnerabilidad ha permanecido por 7 años en iTerm2 MacOS Terminal

Autor: I. Stepanenko

Fecha: Monday 21st of October 2019 10:39:58 AM



Se descubrió una vulnerabilidad crítica de ejecución remota de código que se ha mantenido por 7 años en la aplicación del emulador de terminal iTerm2 MacOS, uno de los reemplazos de código abierto más populares para la aplicación de terminal incorporada de Mac.

Rastreada como CVE-2019-9535, la vulnerabilidad en iTerm2 fue descubierta como parte de una auditoría de seguridad independiente financiada por el Programa de Soporte de Código Abierto de Mozilla (MOSS) y realizada para la firma de seguridad cibernética Radically Open Security (ROS).

> “MOSS seleccionó iTerm2 para una auditoría de seguridad porque procesa datos no confiables y es ampliamente utilizado, incluso por objetivos de alto riesgo (como desarrolladores y administradores de sistemas)”, dijo Mozilla.

Según una publicación de blog hecha hoy por Mozilla, la falla RCE reside en la característica de integración tmux de iTerm2, que de ser explotada, podría permitir que un hacker ejecute comandos arbitrarios al proporcionar una salida maliciosa a la terminal.

Como se muestra en el video, los posibles vectores de ataque para esta vulnerabilidad incluyen conectarse a un servidor SSH malicioso controlado por el atacante, usar comandos como *curl* para buscar un sitio web malicioso o usar *tail -f* para seguir un archivo de registro que contiene contenido malicioso.

Además de esto, la falla también se puede activar utilizando utilidades de línea de comandos engañándolos para que impriman contenido controlado por el atacante, lo que eventualmente permite a los hackers ejecutar comandos arbitrarios en la computadora Mac del usuario.

> “Por lo general, esta vulnerabilidad requeriría cierto grado de interacción del usuario, pero debido a que puede explotarse por medio de comandos generalmente considerados seguros, existe un alto grado de preocupación por el impacto potencial”, advierte Mozilla.

La vulnerabilidad afecta a las versiones de iTerm2 hasta 3.3.5, y recientemente se ha parcheado con el lanzamiento de iTerm2 3.3.6, que los usuarios puedes descargar manualmente o buscar actualizaciones dentro del menú de las aplicaciones instaladas.