Se ha detectado en GitHub un indicio de que los investigadores de ciberseguridad siguen siendo blanco de actores maliciosos, al encontrarse un concepto de prueba (PoC) que oculta una puerta trasera con un método persistente *«astuto».*

> *«En este caso, el PoC es un lobo disfrazado de oveja, con intenciones maliciosas bajo la apariencia inofensiva de una herramienta educativa. Actuando como un descargador, silenciosamente vuelca y ejecuta un script bash de Linux, disfrazando sus operaciones como un proceso a nivel de kernel»,* afirmaron los investigadores de Uptycs, Nischay Hegde y Siddartha Malladi.

El repositorio se hace pasar por un PoC para CVE-2023-35829, una vulnerabilidad recientemente revelada de alta gravedad en el kernel de Linux. Desde entonces ha sido retirado, pero no antes de ser bifurcado 25 veces. Otra PoC compartida por la misma cuenta, ChriSanders22, para CVE-2023-20871, un error de escalada de privilegios que afecta a VMware Fusion, fue bifurcado dos veces.

Uptypcs también identificó un segundo perfil en GitHub que contiene un falso PoC para CVE-2023-35829. Aún está disponible al momento de escribir esto y ha sido bifurcado 19 veces. Un examen más detallado del historial de confirmaciones muestra que los cambios fueron realizados por ChriSanders22, lo que sugiere que fue bifurcado del repositorio original.

Se ha descubierto una puerta trasera que viene con una amplia variedad de capacidades para robar datos sensibles de equipos comprometidos, así como permitir que un actor de amenazas obtenga acceso remoto al agregar su clave SSH al archivo .ssh/authorized_keys.

> *«El PoC tiene la intención de que ejecutemos un comando make, que es una herramienta de automatización utilizada para compilar y construir ejecutables a partir de archivos de código fuente. Sin embargo, dentro del archivo Makefile se encuentra un fragmento de código que construye y ejecuta el malware. El malware crea y ejecuta un archivo llamado kworker, que agrega la ruta*

> *$HOME/.local/kworker en $HOME/.bashrc, estableciendo así su persistencia»,* explicaron los investigadores.

Este hallazgo se produce casi un mes después de que VulnCheck descubriera varias cuentas falsas en GitHub haciéndose pasar por investigadores de seguridad para distribuir malware bajo la apariencia de exploits PoC para software popular como Discord, Google Chrome, Microsoft Exchange Server, Signal y WhatsApp.

Se recomienda a los usuarios que hayan descargado y ejecutado los PoCs que anulen las claves SSH no autorizadas, eliminen el archivo kworker, borren la ruta kworker del archivo bashrc y verifiquen /tmp/.iCE-unix.pid en busca de posibles amenazas.

> *«Aunque puede ser difícil distinguir entre PoCs legítimos y engañosos, adoptar prácticas seguras como probar en entornos aislados (por ejemplo, máquinas virtuales) puede proporcionar una capa adicional de protección»,* señalaron los investigadores.