Ubuntu y otras distribuciones de Linux tienen una vulnerabilidad escalada muy peligrosa que podría permitir que un atacante local o un programa malicioso obtenga privilegios de root y control total del sistema.

Dicha vulnerabilidad se apodó como «Dirty_Sock», y se identifica como CVE-2019-7304, fue descubierta por el investigador de seguridad Chris Moberly, quien se lo reveló a Canonical, el fabricante de Ubuntu, a finales del mes pasado.

La vulnerabilidad reside en la API REST, para el servicio snapd, un sistema universal de empaquetado de Linux que hace que una aplicación sea compatible para varias distribuciones de Linux sin la necesidad de realizar modificaciones.

Snap es construido por Canonical, viene instalado de forma predeterminada en todas las versiones de Ubuntu y también es utilizado por otras distribuciones de Linux, incluyendo Debian, OpenSUSE, Arch Linux, Solus y Fedora.

Los paquetes Snap son básicamente aplicaciones comprimidas junto con sus dependencias que incluyen instrucciones sobre cómo ejecutar e interactuar con otro software en distintos sistemas Linux para escritorio, nube e Internet de las cosas.

Snap aloja localmente un servidor web (socket UNIX_AF) para ofrecer una lista de API RESTful que ayudan al servicio a realizar algunas acciones en el sistema operativo. Estas API REST vienen con control de acceso para definir permisos a nivel de usuario para tareas específicas. Algunas API potentes solo están disponibles para usuarios root, mientras que otras pueden ser accedidas por usuarios con pocos privilegios.

Según Moberly, una falla en la forma en que el mecanismo de control de acceso verifica el UID asociado con cualquier solicitud realizada a un servidor permite a los atacantes sobrescribir la variable UID y acceder a cualquier función de API, incluidas aquellas que están restringidas para el usuario root.

> *«Las versiones de Snapd 2.28 a 2.37 validaron y analizaron incorrectamente la dirección del socket remoto al realizar controles de acceso en su socket UNIX. Un atacante local podría utilizar esto para acceder a las API de socket privilegiadas y obtener privilegios de administrador»,* explica Ubuntu en un aviso.

Sin embargo, es necesario tener en cuenta que, dado que Dirty Sock aprovecha el defecto de escalamiento de privilegios locales, no permite que los piratas informáticos pongan en peligro un sistema Linux vulnerable de forma remota.

Moberly también lanzó dos exploits de pruebas de concepto (PoC) en GitHub, uno de los cuales requiere una conexión SSH, mientras que el otro es capaz de descargar un complemento malicioso al abusar de dicha API.

Canonical lanzó la versión Snapd 2.37.1 esta semana para abordar la vulnerabilidad, Ubuntu y otras distribuciones importantes de Linux ya lanzaron una versión fija de sus paquetes.

Se remienda a los usuarios de Linux que actualicen sus versiones vulnerables lo más pronto posible.