Microsoft reveló el martes dos vulnerabilidades de escalada de privilegios en el sistema operativo Linux, que podrían permitir a los hackers realizar una serie de actividades maliciosas.

Llamadas colectivamente como Nimbuspwn, las vulnerabilidades *«pueden encadenarse para obtener privilegios de root en los sistemas Linux, lo que permite a los atacantes implementar cargas útiles, como una puerta trasera raíz, y realizar otras acciones maliciosas a través de la ejecución arbitraria de código raíz»,* dijo Jonathan Bar Or, de Microsoft 365 Defender Research Team.

Además, las vulnerabilidades, rastreadas como CVE-2022-29799 y CVE-2022-29800, también podrían armarse como un vector para el acceso root para implementar amenazas más sofisticadas como el ransomware.

Las vulnerabilidades tienen sus raíces en un componente de systemd llamado networkd-dispatcher, un programa daemon para el servicio del sistema del administrador de red que está diseñado para enviar cambios de estado de la red.

De forma específica, se relacionan con una combinación de fallas de recorrido de directorio (CVE-2022-29799), carrera de enlace simbólico y fallas de tiempo de verificación a tiempo de uso (CVE-2022-29800), lo que lleva a un escenario en el que un adversario que tiene el control de un servicio D-Bus no autorizado puede plantar y ejecutar puertas traseras maliciosas en los puntos finales comprometidos.

Se recomienda a los usuarios de networkd-dispatcher que actualicen sus instancias a la última versión para mitigar el potencial que surge de la explotación de las vulnerabilidades.

> *«El creciente número de vulnerabilidades en los entornos Linux enfatiza la necesidad de un fuerte monitoreo del sistema operativo de la plataforma y sus componentes»*, dijo Bar Or.

> *«Este bombardeo constante de ataques cibernéticos que abarca una amplia gama de plataformas, dispositivos y otros dominios enfatiza la necesidad de un enfoque de gestión de vulnerabilidades integral y proactivo que pueda identificar y mitigar aún más los exploits y problemas previamente desconocidos»,* agregó.