Un serio problema de escalada de privilegios que afecta a MikroTik RouterOS podría ser aprovechado por actores maliciosos remotos para ejecutar código arbitrario y apoderarse de los dispositivos vulnerables.

Catalogado como CVE-2023-30799 (puntuación CVSS: 9.1), se espera que el problema ponga en riesgo de explotación a unos 500.000 y 900.000 sistemas RouterOS a través de sus interfaces web y/o Winbox, respectivamente, según reveló VulnCheck en un informe del martes.

> *«El CVE-2023-30799 requiere autenticación. De hecho, la vulnerabilidad en sí es una simple escalada de privilegios de administrador a 'super-administrador' que resulta en el acceso a una función arbitraria. Adquirir credenciales para los sistemas RouterOS es más fácil de lo que uno podría esperar»*, dijo el investigador de seguridad Jacob Baines.

Esto se debe a que el sistema operativo Mikrotik RouterOS no ofrece ninguna protección contra los ataques de fuerza bruta de contraseñas y se envía con un usuario «admin» predeterminado y conocido, cuya contraseña es una cadena vacía hasta octubre de 2021, momento en el que se solicitó a los administradores que actualizaran las contraseñas en blanco con el lanzamiento de RouterOS 6.49.

Se dice que el CVE-2023-30799 fue originalmente divulgado por Margin Research como un exploit llamado FOISted sin un identificador CVE adjunto en junio de 2022. Sin embargo, el agujero de seguridad no fue solucionado hasta el 13 de octubre de 2022, en la versión estable de RouterOS 6.49.7 y el 19 de julio de 2023, para la versión a largo plazo de RouterOS 6.49.8.

VulnCheck señaló que un parche para el árbol de lanzamiento a largo plazo sólo estuvo disponible después de que se pusiera en contacto directamente con el proveedor y *«publicara nuevos exploits que atacaban una gama más amplia de hardware MikroTik».*

Una prueba de concepto (PoC) ideada por la empresa muestra que es posible derivar una nueva cadena de exploits basada en la arquitectura MIPS a partir de FOISted y obtener una shell root en el router.

> *«Dada la larga historia de RouterOS de ser un objetivo APT, combinada con el hecho de que FOISted se lanzó hace más de un año, tenemos que asumir que no somos el primer grupo en averiguarlo»*, señaló Baines.

> *«Lamentablemente, la detección es casi imposible. Las interfaces web y Winbox de RouterOS implementan esquemas de cifrado personalizados que ni Snort ni Suricata pueden descifrar e inspeccionar. Una vez que un atacante está establecido en el dispositivo, puede hacerse fácilmente invisible para la interfaz de usuario de RouterOS».*

Con las fallas en los routers Mikrotik explotadas para arrear los dispositivos en botnets distribuidos de denegación de servicio (DDoS) como Mēris y usarlos como proxies de comando y control, se recomienda a los usuarios que parcheen la falla actualizando a la última versión (6.49.8 o 7.x) lo antes posible.

Los consejos de mitigación incluyen eliminar las interfaces administrativas MikroTik de Internet, limitar las direcciones IP desde las que los administradores pueden iniciar sesión, deshabilitar las interfaces Winbox y web, y configurar SSH para usar claves públicas/privadas y deshabilitar las contraseñas.