BOLETÍN DE ALERTA

Boletín Nro.: 2023-35
Fecha de publicación: 27/07/2023
Tema: Vulnerabilidad crítica de escalamiento de privilegios en MikroTik RouterOS

Software afectado:

- MikroTik RouterOS, versión 6.48.6 y anteriores a 6.49.7.

Descripción:

Se ha reportado un nuevo aviso de seguridad sobre una vulnerabilidad de nivel crítico que afecta a MikroTik RouterOS, que permitiría a un atacante remoto autenticado a través de una cuenta administrador existente en el sistema operativo, realizar escalamiento de privilegios de *super-admin* en el sistema afectado, permitiendo a los atacantes obtener el control total del dispositivo sin ser detectados.

La vulnerabilidad ha sido identificada como CVE-2023-30799, de severidad "Crítica", con una puntuación asignada de 9.1. Esta vulnerabilidad se debe a una falla de seguridad en la administración de privilegios de MikroTik RouterOS. Esto permitiría a un atacante autenticado a través de una cuenta administradora válida realizar el envío de una solicitud especialmente diseñada, derivando en un escalamiento de privilegios de un usuario *admin* a *super-admin* en la interfaz de administración *Winbox* o *HTTP*.

Super-admin no es un privilegio otorgado a los administradores normales, es un privilegio que se otorga a ciertos componentes del software (específicamente, en este caso, para cargar bibliotecas en la interfaz web) y no a los usuarios finales. Al escalar a *super-admin*, el atacante puede llegar a acceder a rutas de códigos internos del dispositivo, permitiendo controlar las llamadas a funciones, es decir, tomar el control total del dispositivo y poder permanecer activos en el mismo sin ser detectados.

Se recomienda tomar acción de forma inmediata, debido a la baja complejidad que se requiere por parte de un atacante para ganar acceso de administrador en los dispositivos afectados, como técnicas de ataques de fuerza bruta para adivinar la credencial del usuario admin, el cual no exige complejidad para la misma.

Impacto:

La explotación exitosa de esta vulnerabilidad permitiría a un atacante autenticado realizar escalamiento de privilegios como usuario *admin* a *super-admin* y ejecutar código arbitrario en el sistema afectado.

Solución:

Recomendamos actualizar a la última versión provista por el fabricante en el siguiente enlace:

- https://mikrotik.com/download
- https://mikrotik.com/download/changelogs/long-term-release-tree

Adicionalmente, sugerimos seguir los siguientes pasos de mejores prácticas:

- Restringir la administración remota a través de Internet.
- Restringir las direcciones *IP* de inicio de sesión de acuerdo a una lista predefinida.
- Deshabilitar el acceso a través de *Winbox* y solo usar *SSH*.
- Proteger el acceso remoto por *SSH* para usar claves públicas/privadas en lugar de contraseñas.

Información adicional:

- https://www.bleepingcomputer.com/news/security/super-admin-elevation-bug-puts-900-000-mikrotik-devices-at-risk/
- https://www.redpacketsecurity.com/mikrotik-routeros-privilege-escalation-cve-2023-30799/
- https://nvd.nist.gov/vuln/detail/CVE-2023-30799
- https://vulncheck.com/advisories/mikrotik-foisted
- https://mikrotik.com/download
- https://mikrotik.com/download/changelogs/long-term-release-tree