

Boletín de alerta

Boletín Nro.: 97

Fecha de publicación: 07/09/2026

Tema: Alerta 2026-97 Zero-day en MikroTik RouterOS explotado activamente vía SSH expuesto a Internet

Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Producto	Rango afectado	Versión corregida mínima
MikroTik RouterOS 6	6.0.0 hasta antes de 6.49.21	6.49.21
MikroTik RouterOS 7 Long-term	7.0.0 hasta antes de 7.23.4	7.23.4; se recomienda 7.23.5 por corrección adicional de regresión
MikroTik RouterOS 7 Stable	7.24 hasta antes de 7.24.2	7.24.2
MikroTik RouterOS 7 Development	No listado en el rango de CERT	7.25beta3

Descripción

Recientemente CERT Polska y MikroTik publicaron una alerta de seguridad sobre **seis vulnerabilidades ZeroDay** en **MikroTik RouterOS**, incluyendo fallas que permiten bypass de autenticación SSH, apertura de canales SSH no autenticados, lectura arbitraria de archivos mediante WebFig, elevación de privilegios, suplantación de certificados TLS y denegación de servicio. La publicación incluye **CVE-2026-67276, CVE-2026-67277, CVE-2026-67278, CVE-2026-67279, CVE-2026-67281 y CVE-2026-66060**, con severidades que van de **Alta a Crítica**.

Las vulnerabilidades con mayor impacto son **CVE-2026-67276**, que permite suplantar la autenticación SSH de usuarios con claves RSA autorizadas; **CVE-2026-67279**, que permite abrir un canal SSH y ejecutar solicitudes sin completar autenticación; y **CVE-2026-67281**, que permite leer archivos protegidos desde el endpoint WebFig /jsproxy, potencialmente incluyendo configuraciones y credenciales almacenadas en el router. La combinación de estas fallas puede permitir a un atacante remoto no autenticado obtener acceso al dispositivo, extraer información sensible, modificar archivos de configuración o elevar privilegios.

CERT Polska confirmó la explotación activa de una cadena de dos vulnerabilidades, denominada **MikroTrick**, contra routers MikroTik que tienen SSH accesible desde Internet. Aunque el fabricante y CERT

han confirmado la actividad, no se han revelado públicamente los dos CVE concretos que conforman dicha cadena; por ello, se recomienda considerar todos los sistemas RouterOS dentro de los rangos vulnerables como prioritarios para actualización y revisión de compromiso.

Las fallas divulgadas son las siguientes:

CVE	Severidad / tipo	Impacto principal
CVE-2026-67276 (CVSSv4 9.2)	Validación criptográfica incorrecta, CWE-347	Permite falsificar autenticación SSH como un usuario autorizado con clave RSA, sin disponer de la clave privada.
CVE-2026-67277 (CVSSv4 8.8)	Ausencia de autenticación en función crítica, CWE-306	Permite iniciar pruebas UDP IPv4 no autenticadas mediante btest; puede filtrar datos no inicializados del buffer del kernel y provocar reinicios del kernel por un error de tamaño de paquete.
CVE-2026-67278 (CVSSv4 6.3)	Validación criptográfica incorrecta, CWE-347	Permite falsificar certificados durante validación X.509 y suplantar servidores TLS si el atacante controla o redirige conexiones salientes del router.
CVE-2026-67279 (CVSSv4 6.9)	Flujo de trabajo incorrecto, CWE-341	Permite abrir un canal de sesión SSH sin autenticación y ejecutar solicitudes que habilitan creación, sobrescritura o reconstrucción de archivos en el espacio administrado de RouterOS.
CVE-2026-67281 (CVSSv4 8.7)	Acceso a puntero no inicializado, CWE-324	Permite lectura no autenticada de archivos mediante WebFig /jsproxy, incluyendo archivos propiedad de root y potencialmente almacenes de configuración con credenciales.
CVE-2026-86060 (CVSSv4 9.2)	Inyección de argumentos, CWE-38	Permite alterar la máscara de políticas de RouterOS y elevar privilegios a través de una debilidad en el procesamiento de nombres de usuario durante el inicio de sesión SSH.

Solución

Actualizar RouterOS de inmediato a una versión corregida y soportada:

- RouterOS 6: 6.49.21 o posterior.
- RouterOS 7 Long-term: 7.23.5 o posterior.
- RouterOS 7 Stable: 7.24.2 o posterior.

<https://help.mikrotik.com/docs/spaces/ROS/pages/328142/Upgrading+and+installation>

Revisar el estado de seguridad del equipo después de actualizar mediante:

/system/device-mode/print

RouterOS puede marcar el dispositivo como Flagged si detecta configuraciones sospechosas durante las comprobaciones de inicio.

- Revisar registros y configuración en busca de:
- Usuarios locales desconocidos, especialmente cuentas privilegiadas denominadas ops.
- Eventos de creación de cuentas con el indicador ssh:-2@.
- Scripts, *scheduler jobs*, reglas de firewall, NAT, VPN, proxy, DNS o túneles no reconocidos.
- Archivos inesperados, configuraciones modificadas o cambios administrativos fuera de ventana de mantenimiento.

Recomendaciones adicionales:

- Mantener las reglas de firewall por defecto de MikroTik, que normalmente bloquean la exposición pública de puertos de administración en dispositivos domésticos mientras no hayan sido modificadas.
- Establecer acceso de administración por una red de gestión dedicada, VPN administrativa o *jump host*, en lugar de exponer SSH, WinBox, WebFig o API directamente a Internet.
- Aplicar listas allowed-address para las cuentas administrativas y limitar el acceso a servicios de gestión usando reglas de firewall de entrada.
- Deshabilitar servicios no utilizados, especialmente btest, FTP, Telnet, HTTP, API y APIs legacy.
- Centralizar logs de RouterOS en un servidor remoto/SIEM, de modo que la evidencia permanezca disponible aun cuando el atacante manipule o reinicie el dispositivo.

Validar regularmente la configuración mediante respaldos controlados y comparaciones de cambios; tratar modificaciones no autorizadas en dispositivos perimetrales como un posible incidente de seguridad.

Información adicional:

- <https://cert.pl/en/posts/2026/09/mikrotik-routeros-cve/>
- <https://thehackernews.com/2026/09/attackers-hijack-mikrotik-routers.html>