

Boletín de alerta

Boletín Nro.: 83

Fecha de publicación: 05/08/2026

Tema: Alerta 2026-83 Vulnerabilidad DoS crítica en MikroTik RouterOS

Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- MikroTik RouterOS – todas las versiones
- MikroTik Cloud Hosted Router – todas las versiones

Descripción

Se ha publicado ~~CVE-2026-16347~~ (CVSS 8.8 – Alto) en MikroTik RouterOS y Cloud Hosted Router: una falla de autenticación sin rate limiting efectivo que permite a un atacante realizar fuerza bruta contra la API de administración hasta obtener credenciales válidas. No existe parche disponible a la fecha; ZoomEye identifica más de 934.000 instancias expuestas globalmente.

MikroTik RouterOS es el sistema operativo propietario de MikroTik utilizado en routers, switches y dispositivos de red ampliamente desplegados en entornos empresariales, ISPs, infraestructura crítica e industrial a nivel global. El 28 de julio de 2026 fue publicada la vulnerabilidad ~~CVE-2026-16347~~ (CVSS 4.0: **8.7 / CVSS 3.1: 8.8 – Alto**), clasificada como **CWE-307 (Improper Restriction of Excessive Authentication Attempts)**, que afecta al manejo de autenticación en la **API de administración** de RouterOS y Cloud Hosted Router en **todas las versiones disponibles**. CISA publicó un advisory específico sobre esta vulnerabilidad, y el equipo de ZoomEye identificó más de **934.800 instancias expuestas globalmente** buscables mediante el filtro vul.cve=»CVE-2026-16347»o el dork app=»MikroTik RouterOS».

- ~~CVE-2026-16347~~ – **Improper Restriction of Excessive Authentication Attempts en RouterOS API (CVSS 4.0: 8.7 / CVSS 3.1: 8.8 – Alto)**

El sistema de autenticación de la API de MikroTik RouterOS no implementa controles efectivos contra intentos de login excesivos. Concretamente:nvd.nist+2

- No existe **rate limiting** significativo para intentos fallidos de autenticación.
- No hay mecanismo de **account lockout** o bloqueo de cuenta tras múltiples fallos.
- No se aplican **restricciones por IP de origen** para intentos repetidos.
- En algunas versiones existe un **delay fijo por conexión**, pero puede ser eludido fácilmente mediante **sesiones concurrentes**, lo que permite mantener un volumen alto de intentos distribuidos entre

Como resultado, un atacante con acceso de red a la API de administración puede ejecutar ataques de **fuerza bruta, password spraying o credential stuffing** a gran escala sin que el dispositivo oponga resistencia efectiva, hasta obtener credenciales válidas de administrador. La explotación exitosa otorga acceso administrativo completo al dispositivo, incluyendo modificación de configuración, acceso a credenciales almacenadas, establecimiento de persistencia y uso del dispositivo como pivote hacia la red interna.

El riesgo es especialmente elevado cuando los servicios de administración (API, WinBox, WebFig) están expuestos directamente a Internet o redes no confiables, lo que aplica a una fracción significativa de las más de 934.000 instancias identificadas por ZoomEye.

Mitigación

A la fecha de publicación de este boletín **no existe parche oficial disponible** de MikroTik para CVE-2026-16347. Las siguientes medidas de mitigación deben aplicarse de forma inmediata:

1. Restringir el acceso a la API y servicios de administración

Limitar el acceso a los servicios de gestión (API port 8728/8729, WinBox port 8291, WebFig/HTTPS, SSH, Telnet) exclusivamente a IPs de administración confiables mediante firewall o ACLs en IP Services.

2. Deshabilitar servicios de administración no necesarios

Deshabilitar Telnet, FTP, HTTP WebFig sin cifrado, API plano (sin SSL), proxy, SOCKS, UPnP y DNS remoto si no son estrictamente requeridos.

3. Implementar controles de acceso adicionales

Usar listas blancas de IP en cada servicio de administración habilitado en IP Services Allowed From.

4. Habilitar autenticación de dos factores donde sea posible

Configurar reglas de firewall adicionales que restrinjan el acceso a la API solo desde segmentos de red de gestión.

5. Verificar exposición en ZoomEye

Identificar si dispositivos de la organización aparecen expuestos usando el filtro:

vul.cve=»CVE-2026-16347»o el dork app=»MikroTik RouterOS»

Enlace de búsqueda: <https://www.zoomeye.hk/searchResult?q=vul.cve%3D%22CVE-2026-16347%22>

6. Revisar logs de autenticación

Buscar en los logs del router intentos de autenticación fallidos masivos o desde IPs desconocidas como indicador de explotación en curso.

Solución

MikroTik no ha publicado a la fecha un parche oficial específico para CVE-2026-16347. Se recomienda:

Producto	Estado del parche	Acción recomendada
----------	-------------------	--------------------

MikroTik RouterOS – todas las versiones

Sin parche disponible a la fecha

Aplicar mitigaciones listadas arriba y monitorear el canal de seguridad de MikroTik

MikroTik Cloud Hosted Router – todas las versiones

Sin parche disponible a la fecha

Aplicar mitigaciones listadas arriba y monitorear el canal de seguridad de MikroTik

Monitorear el portal de seguridad oficial de MikroTik para la publicación del parche:

<https://mikrotik.com/supportsec>

Información adicional:

- NVD – CVE-2026-16347
<https://nvd.nist.gov/vuln/detail/CVE-2026-16347>
- CISA – Advisory CVE-2026-16347
<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- Secarma – MikroTik routers vulnerable to rapid password brute forcing
<https://secarma.com/29-07-2026-mikrotik-authentication-vulnerability>
- Mallory.ai – Brute-forceable API Authentication in MikroTik RouterOS
<https://mallory.ai/vulnerabilities/CVE-2026-16347>
- ZoomEye – Búsqueda de instancias expuestas (CVE-2026-16347)
<https://www.zoomeye.hk/searchResult?q=vul.cve%3D%22CVE-2026-16347%22>
- Foro MikroTik – Discusión técnica CVE-2026-16347
<https://forum.mikrotik.com/t/euvs-2026-50017-cve-2026-16347-ghsa-8v62-p5rj-72x6-which-routers-version-does-fix-that/271934>
- MikroTik Security Portal
<https://mikrotik.com/supportsec>