Nro. Alerta:	AL-2026-046	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	18-sep-2026	Vulnerabilidades críticas en MikroTik RouterOS explotadas activamente – CVE-2026-67276, CVE-2026-86060 y CVE-2026-67277	Pág.: **1** of **5**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de Incidente: Explotación de vulnerabilidades / Compromiso de dispositivos de red
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- Vulnerabilidades críticas en MikroTik RouterOS explotadas activamente – CVE-2026-67276, CVE-2026-86060 y CVE-2026-67277 - Figura referencial

El CERT Polska (Equipo de Respuesta a Emergencias Informáticas) de Polonia informó sobre tres vulnerabilidades críticas en MikroTik RouterOS: CVE-2026-67276, relacionada con una omisión de autenticación SSH; CVE-2026-86060, que permite la manipulación de privilegios de sesión SSH mediante un nombre de usuario manipulado; y CVE-2026-67277, que puede provocar divulgación de memoria y fallo del sistema mediante una prueba de ancho de banda. La explotación conjunta de estas vulnerabilidades podría permitir a un atacante tomar el control total del dispositivo sin necesidad de autenticación, siempre que este tenga habilitado el acceso remoto mediante SSH.

III. INTRODUCCIÓN

CERT Polska descubrió y divulgó las siguientes vulnerabilidades: CVE-2026-67276, una vulnerabilidad de omisión de autenticación SSH causada por una validación incompleta de las claves públicas RSA; y CVE-2026-86060, una vulnerabilidad de escalada de privilegios SSH debido a un manejo inadecuado de nombres de usuario especialmente diseñados. Ambas fallas permitirían a un atacante tomar el control de dispositivos con servicios SSH expuestos a Internet.

La cadena de ataque 0-day de ambas vulnerabilidades contra dispositivos MikroTik RouterOS accesibles desde Internet que está siendo explotada ha sido denominada MikroTrick.

En cuanto a la vulnerabilidad CVE-2026-67277, esta afecta al servicio de prueba de ancho de banda de RouterOS y permite a atacantes no autenticados divulgar información de la memoria del kernel o provocar el bloqueo y reinicio remoto del enrutador.

CERT Polska confirma que los atacantes están explotando esta combinación de vulnerabilidades para tomar el control total de dispositivos cuyo servicio SSH es accesible desde redes públicas.

IV. VECTOR DE ATAQUE

CVE-2026-67276 posee una severidad CRÍTICA, con una puntuación CVSS de 9.2 y el siguiente vector: CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H

RouterOS no verificaba correctamente las claves públicas utilizadas para la autenticación SSH; en concreto, no comparaba la clave pública RSA completa asignada a un usuario. Un atacante que conociera el nombre de usuario y el módulo público de la clave del usuario podía crear una clave diferente e iniciar sesión mediante SSH sin poseer la clave privada correspondiente. Los privilegios obtenidos eran equivalentes a los de la cuenta objetivo.

CVE-2026-86060 posee una severidad CRÍTICA, con una puntuación CVSS de 9.2 y el siguiente vector: CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H

RouterOS no gestionaba correctamente los nombres de usuario que comenzaban con un carácter no permitido en el mecanismo de inicio de sesión SSH. Mediante un nombre de usuario manipulado, un atacante podía elevar sus privilegios. La sesión resultante tenía privilegios administrativos completos en el sistema RouterOS.

CVE-2026-67277 posee una severidad ALTA, con una puntuación CVSS de 8.8 y el siguiente vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N

El servicio de prueba de ancho de banda permitía que una conexión no autenticada accediera a una funcionalidad que debía estar restringida a usuarios autenticados. Esta condición, combinada con dos fallas adicionales relacionadas con la divulgación de datos no inicializados del búfer de paquetes y un desbordamiento negativo de enteros durante la validación del tamaño, podía permitir la exposición de información de la memoria del kernel o provocar una denegación de servicio (DoS) remota, ocasionando el bloqueo y reinicio del dispositivo.

La mayoría de los ataques observados y reportados por CERT Polska procedían de 82.192.72 [.]4, una dirección IP de Leaseweb que alojaba un binario de BusyBox una versión para MIPS de 2010, idéntica al binario precompilado oficial de BusyBox 1.16.1, junto con otros tres archivos: ftpsrv.py, launch.sh y serve.py. También se ha asociado a la campaña una segunda dirección IP: 103.102.31 [.]18.

Los administradores de seguridad pueden detectar los ataques buscando entradas específicas en los registros, como intentos fallidos de inicio de sesión que muestran el nombre de usuario “-2”, el cual no corresponde a una cuenta válida y no debería aparecer en los registros durante el funcionamiento normal. Un ataque exitoso puede aparecer en el historial de /system como ssh:-2@<IP>, seguido de una acción como la creación de un usuario, la adición de una clave SSH, la modificación de las reglas del cortafuegos o la habilitación de un proxy o túnel.

Además, un usuario en un foro polaco sobre ciberseguridad publicó registros que mostraban intentos de explotación y CERT Polska confirmó que se produjeron ataques exitosos, entre ellos la creación de una cuenta denominada «ops».

V. IMPACTO

Producto	Versiones afectadas
MikroTik RouterOS	7.25beta3
MikroTik RouterOS	7.24.2
MikroTik RouterOS	7.23.4
MikroTik RouterOS	7.23.5
MikroTik RouterOS	6.49.21

Tabla 1.- Versiones afectadas - Vulnerabilidades críticas en MikroTik RouterOS explotadas activamente – CVE-2026-67276, CVE-2026-86060 y CVE-2026-67277

VI. INDICADORES DE COMPROMISO

Dirección IP
82.192.72 [.]4
103.102.31 [.]18

Tabla 2.- Direcciones IP - Vulnerabilidades críticas en MikroTik RouterOS explotadas activamente – CVE-2026-67276, CVE-2026-86060 y CVE-2026-67277

SHA-256	Archivo
6e95f70fdbabb57881b3f5b2c8465d4b17ba901100704efb1278bb3386e6729d	ftpsrv.py
972b474b896f9fac3cd6b5b8476b410b8f39fbedee8a3b0c745d6e3b328d7dcd	launch.sh
6dca83338d60467b65b7789d4d59754e40a7aaa36f40ea2da57538367ac9b89e	serve.py

Tabla 3.- SHA-256 - Vulnerabilidades críticas en MikroTik RouterOS explotadas activamente – CVE-2026-67276, CVE-2026-86060 y CVE-2026-67277

Indicador
Intento de inicio de sesión mediante SSH con el usuario -2.
Registro de actividad como ssh:-2@<IP>.
Creación de una cuenta denominada ops con privilegios elevados.

Tabla 4.- Indicadores -Vulnerabilidades críticas en MikroTik RouterOS explotadas activamente – CVE-2026-67276, CVE-2026-86060 y CVE-2026-67277

VII. RECOMENDACIONES

- Actualizar RouterOS a una versión corregida: 7.25beta3, 7.24.2, 7.23.4 o 6.49.21, según corresponda.
- Revisar los registros y la configuración del dispositivo para identificar usuarios, claves SSH, scripts o cambios no autorizados.

- Mientras se aplica la actualización, restringir o deshabilitar los servicios expuestos a Internet, especialmente SSH, WWW/WWW-SSL y el servidor de prueba de ancho de banda.
- Evitar conexiones TLS y el uso de los clientes SSH integrados desde dispositivos que aún no hayan sido actualizados.
- En caso de detectar indicios de compromiso, aislar el dispositivo, preservar los registros y la configuración antes de reiniciarlo y notificar al CSIRT correspondiente.
- Si se confirma el compromiso, restaurar el dispositivo a una configuración confiable, cambiar contraseñas y claves, y evitar restaurar directamente copias de seguridad de un equipo comprometido.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

CERT.PL. (2026). *Vulnerabilities in MikroTik RouterOS actively exploited.* https://cert.pl/en/posts/2026/09/vulnerabilities-in-mikrotik-routeros-actively-exploited/

SECURITY AFFAIRS. (2026). *Your MikroTik Router May Already Be Compromised: Look for SSH User 2.* https://securityaffairs.com/198538/security/your-mikrotik-router-may-already-be-compromised-look-for-ssh-user-2.html?amp

STARTUP FORTUNE. (2026). *MikroTik Routers Are Being Hijacked Through a Flaw Patched Days Ago.* https://startupfortune.com/mikrotik-routers-are-being-hijacked-through-a-flaw-patched-days-ago/

BLEEPINGCOMPUTER. (2026). *Hackers Exploit New MikroTik RouterOS Flaws to Hijack Routers.* https://www.bleepingcomputer.com/news/security/hackers-exploit-new-mikrotik-routeros-flaws-to-hijack-routers/amp/