



Wiceprezes Rady Ministrów Minister Cyfryzacji

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa
Krzysztof Gawkowski

DC.WAC.5555.106.2026
Warszawa, 01 października 2026 r.

Rekomendacja Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa

nr 2026/33/5

dotycząca podatności w oprogramowaniu MikroTik RouterOS

Rekomenduję podmiotom krajowego systemu cyberbezpieczeństwa¹ niezwłoczne zaktualizowanie oprogramowania MikroTik RouterOS co najmniej do wersji:

- 7.25 beta 3,
- 7.24.2,
- 7.23.4,
- 6.49.21.

Ze względu na wykorzystywanie podatności przez atakujących, rekomendowana jest weryfikacja, czy urządzenia zostały skompromitowane, zgodnie z instrukcją udostępnioną przez producenta <https://manual.mikrotik.com/docs/system-information-and-utilities/device-mode/#flagged-status>

Dodatkowo rekomendowane jest wyłączenie usług SSH, WWW/WWW-SSL, WinBox oraz serwera bandwidth-test albo zablokowanie do nich dostępu ze wszystkich adresów spoza zaufanych sieci zarządzających.

Podatności CVE-2026-67276, CVE-2026-67277, CVE-2026-67278, CVE-2026-67279, CVE-2026-67281, CVE-2026-86060 dotyczące oprogramowania MikroTik RouterOS umożliwiają całkowite obejście mechanizmu uwierzytelnienia i uzyskanie pełnej kontroli nad RouterOS. Połączenie podatności CVE-2026-67276, umożliwiającej uwierzytelnienie za pomocą spreparowanego klucza RSA, oraz CVE-2026-86060, pozwalającej na eskalację uprawnień, stanowi poważne zagrożenie dla urządzeń MikroTik dostępnych z sieci Internet. Wykorzystanie obu podatności w ramach jednego łańcucha ataku może prowadzić do uzyskania pełnej kontroli nad urządzeniem.

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa przeprowadził konsultację w powyższym zakresie z CSIRT NASK, CSIRT GOV oraz CSIRT MON, na podstawie której została potwierdzona możliwość wystąpienia incydentu krytycznego w przypadku niezastosowania się do powyższej rekomendacji. Tym samym stwierdza się, że stosowanie oprogramowania z ww. podatnościami ma negatywny wpływ na bezpieczeństwo publiczne i istotny interes bezpieczeństwa państwa.

Podmiot krajowego systemu cyberbezpieczeństwa może wnieść zastrzeżenia do niniejszej rekomendacji na zasadach określonych w ustawie o KSC².

Krzysztof Gawkowski

Wiceprezes Rady Ministrów

¹ Podmioty, o których mowa w art. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2026 r. poz. 20 z późn. zm.), dalej jako: „ustawa o KSC”.

² Art. 33 ust. 5 ustawy o KSC.

Minister Cyfryzacji
Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa
/dokument podpisany elektronicznie/