



NO.DG-II/ Cyber Advisory/4/111/2023
GOVERNMENT OF SINDH
SCIENCE & INFORMATION TECHNOLOGY DEPARTMENT

Karachi, Dated: 17th September 2026

To

1. The Chairman, Planning & Development Board, Govt. of Sindh, Karachi
2. The Chairman, Enquires, Anti-Corruption, Establishment of Sindh, Karachi.
3. The Chairman Chief Minister's Inspection Enquiries and Implementation Team
4. The Chairman Sindh HEC Karachi.
5. The Senior Member Board of Revenue (BOR) Sindh, Karachi.
6. The Additional Chief Secretary, Govt of Sindh _____
7. The Principal Secretary to Governor Sindh, Governor Secretariat, Karachi.
8. The Principal Secretary to Chief Minister Sindh, Chief Minister Secretariat, Karachi.
9. The Administrative Secretary, Government of Sindh (All). _____
10. The Provincial Ombudsman, Sindh.
11. The Inspector General of Police Sindh, Karachi
12. The Divisional Commissioner (All) in Sindh _____

SUBJECT: CYBERSECURITY ADVISORY ON EXPLOITATION OF MIKROTIK ROUTERS

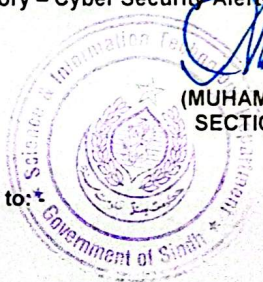
In view of the reported increase in automated brute-force attacks, exploitation attempts, and unauthorized access targeting publicly reachable MikroTik routers, the attached Advisory titled "NCA-42.310826 National CERT Advisory Cybersecurity Alert - MikroTik Router Exploitation" (**Annexure**) has been issued by the National Cyber Emergency Response Team (National CERT).

2. The advisory highlights key threats targeting internet-exposed MikroTik routers, including automated scanning account enumeration, credential brute-forcing, exploitation of vulnerable RouterOS firmware, unauthorized administrative access, configuration manipulation persistence botnet recruitment, and network reconnaissance.

3. MikroTik routers operating outdated or unpatched RouterOS versions, retaining factory-default configurations, using weak administrative credentials, or exposing management services such as Winbox, WebFig, SSH, REST API and SNMP to the public internet may be particularly vulnerable. The advisory provides recommended measures covering RouterOS patching, credential hardening, restriction of remote management access, disabling of unnecessary services, SNMP security, account review, configuration integrity checks, and continuous monitoring.

4. In view of the potential impact of compromised network infrastructure on the confidentiality, integrity, and availability of organizational systems and services, it is requested that the attached Advisory be disseminated to all relevant departments, agencies, and organizations under your administrative control for immediate awareness, assessment, and implementation of the recommended security measures, particularly for internet-facing MikroTik devices.

Annexure: NCA-42.310826 - National CERT Advisory – Cyber Security Alert MikroTik Router


(MUHAMMAD AKBAR KHAN)
SECTION OFFICER (TECH) 17/9/2026


A copy is forwarded for information and necessary action to:-

1. CEO Sindh IT Company.
2. DG(nCERT) NCERT Government of Pakistan
3. PS to Chief Secretary, Sindh.
4. Staff Officer to Secretary, S&IT Department, Government of Sindh.
5. Webmaster S&IT Department to publish on the official website(s).

SECTION OFFICER (TECH)



National Cyber Emergency Response Team

Government of Pakistan



Annexure

NCA-42.310826 – National CERT Advisory

Cybersecurity Alert – MikroTik Router Exploitation

A heightened cybersecurity risk has been identified involving the active exploitation and automated brute-force targeting of publicly reachable MikroTik routers, with particular concern for routers deployed in defense, government, and other sensitive environments. Threat actors are scanning the public IPv4 address space for exposed MikroTik management interfaces and attempting to gain unauthorized administrative access through weak credentials or known vulnerabilities in outdated RouterOS firmware.

The primary risks involve legacy or unpatched RouterOS installations, factory-default configurations, weak administrative passwords, exposed management services, and insecure SNMP configurations. Successfully compromised routers may be incorporated into botnets, abused as traffic proxies, or used as staging points for reconnaissance and further unauthorized access within internal networks.

This advisory outlines the observed attack methods, potentially affected configurations, known vulnerabilities, indicators of exposure, and recommended remediation measures. Organizations are strongly encouraged to assess all internet-facing MikroTik devices and prioritize the patching and hardening of routers exposed to untrusted networks.

DOCUMENT SUMMARY

Advisory ID	NCA-42.310826
Threat Type	Router Exploitation / Credential Brute Force / Unauthorized Access / Botnet Recruitment
Severity	High
Attack Vector	Internet-exposed Winbox, Web/HTTP(S), SSH, SNMP and REST API services
Authentication Required	Depends on vulnerability; brute-force attacks require valid authentication attempts
User Interaction	Not Required for remote exploitation or automated scanning

National Cyber Emergency Response Team (NCERT)

Government of Pakistan

Pak Secretariat, L Block, Islamabad, Pakistan

+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk



National Cyber Emergency Response Team

Government of Pakistan



1. IMPACT ANALYSIS

Compromise of vulnerable or poorly secured MikroTik routers may result in:

- Unauthorized Administrative Access** – Attackers gaining privileged access to router configuration and management functions.
- Network Reconnaissance** – Compromised routers being used to identify internal systems, services, routes, and network infrastructure.
- Botnet Recruitment** – Routers being incorporated into distributed botnets for scanning, proxying, denial-of-service activity, or other malicious operations.
- Traffic Proxying** – Compromised devices being abused to route malicious traffic while concealing the attacker's originating infrastructure.
- Credential Compromise** – Weak or reused administrative credentials being obtained through automated brute-force attacks.
- Persistence** – Attackers modifying users, firewall rules, routing configurations, or scripts to maintain continued access.
- Network Security Bypass** – Unauthorized modification of firewall and routing rules potentially allowing malicious traffic into or through protected networks.
- Service Disruption** – Unauthorized configuration changes potentially affecting network availability and connectivity.
- Sensitive Information Exposure** – Router configurations, network topology, credentials, and other operational information may be exposed.
- Lateral Movement** – A compromised router may provide attackers with a strategic position from which to conduct further attacks against connected systems.

2. THREAT CHARACTERISTICS

Sr. No.	Characteristic	Details
a.	Threat Category	Internet-facing network infrastructure exploitation
b.	Threat Status	Active / Ongoing
c.	Root Cause	Unpatched RouterOS, weak credentials, default configurations and exposed management services
d.	Data Sensitivity	Network configuration, credentials, routing information and operational infrastructure data
e.	Attack Complexity	Low to Medium
f.	Privileges Required	None for certain remote vulnerabilities; administrative credentials may be required for brute-force compromise
g.	Affected Systems	MikroTik routers running vulnerable RouterOS versions or insecure configurations
h.	Primary Management Services	Winbox TCP/8291, HTTP/HTTPS TCP/80/443, SSH TCP/22, SNMP UDP/161/162 and REST API

National Cyber Emergency Response Team (NCERT)

Government of Pakistan

Pak Secretariat, L Block, Islamabad, Pakistan

+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk



National Cyber Emergency Response Team

Government of Pakistan



3. ATTACK METHODOLOGY

Threat actors may conduct the following sequence of activities against publicly reachable MikroTik routers:

- a. **Internet-Wide Scanning:** Attackers scan publicly accessible IPv4 addresses to identify MikroTik devices exposing management services, particularly:
 - Winbox – TCP 8291
 - Web/HTTP(S) – TCP 80/443
 - SSH – TCP 22
 - SNMP – UDP 161/162
 - REST API endpoints
- b. **Account Enumeration:** Attackers may exploit vulnerabilities or response discrepancies to identify valid administrative usernames before attempting authentication.
- c. **Credential Brute Force:** Automated scripts may attempt commonly used or previously compromised passwords against exposed management interfaces. Examples of weak/default credentials include:
 - admin
 - 123456
 - password
 - mikrotik
 - Blank/default passwords
- d. **Exploitation of Vulnerable Firmware:** Where vulnerable RouterOS versions are identified, attackers may attempt to exploit known vulnerabilities to obtain unauthorized access or execute malicious actions.
- e. **Privilege Escalation and Persistence:** Following successful compromise, attackers may modify system users, firewall rules, routing tables, scripts, or other configurations to establish persistence and facilitate further activity.

National Cyber Emergency Response Team (NCERT)

Government of Pakistan

Pak Secretariat, I Block, Islamabad, Pakistan

+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk



National Cyber Emergency Response Team

Government of Pakistan



4. KNOWN VULNERABILITIES

Sr. No.	CVE	Reported Vulnerability / Risk
a.	CVE-2026-7668	Endpoint out-of-bounds read vulnerability affecting legacy RouterOS v6 branches
b.	CVE-2025-10948	Buffer overflow vulnerability reportedly affecting the RouterOS REST API endpoint /rest/ip/address/print, potentially enabling remote code execution
c.	CVE-2024-54772	Winbox account-enumeration vulnerability involving response-size discrepancies that may allow identification of valid usernames
d.	CVE-2022-45315	Legacy RouterOS memory-corruption vulnerability
e.	CVE-2021-3014	Legacy RouterOS Reflected Cross-Site Scripting (XSS) vulnerability affecting the hotspot login page via the target parameter

Note: Organizations should verify the applicability, affected versions, and vendor remediation status of individual CVEs against their deployed RouterOS versions before undertaking remediation.

5. INDICATORS OF EXPOSURE (IoEs)

Organizations should investigate the following indicators on MikroTik routers:

- Repeated failed login attempts against administrative accounts.
- Authentication attempts originating from unusual or previously unseen external IP addresses.
- Unexpected successful logins to Winbox, WebFig, SSH, or other management interfaces.
- Unknown or newly created administrative user accounts.
- Unexpected changes to firewall rules or NAT configurations.
- Unauthorised modifications to routing tables or network routes.
- Unknown or suspicious RouterOS scripts configured for scheduled or persistent execution.
- Unexpected changes to DNS, proxy, or traffic-forwarding configurations.
- Unusual outbound traffic originating from the router.
- Unexpected SNMP exposure or use of default community strings such as public or private.
- Management services accessible from the public internet without appropriate access controls.
- RouterOS versions that are outdated or no longer appropriately patched.

National Cyber Emergency Response Team (NCERT)

Government of Pakistan

Pak Secretariat, L Block, Islamabad, Pakistan

+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk



National Cyber Emergency Response Team

Government of Pakistan



6. REMEDIATION ACTIONS

Sr. No.	Action Category	Specific Actions
a.	RouterOS Patching	Upgrade MikroTik devices to the latest vendor-supported and security-patched RouterOS release
b.	Legacy Devices	Where supported and applicable, patch legacy RouterOS v6 devices to at least v6.49.20
c.	Credential Security	Replace all default, weak, shared or easily guessable passwords with strong, unique credentials
d.	Management Access	Restrict Winbox, WebFig, SSH and REST API access to trusted administrative networks or approved IP addresses
e.	Unused Services	Disable Telnet and other unnecessary management services
f.	Firewall Controls	Apply restrictive input firewall rules to prevent unauthorized access to management interfaces
g.	SNMP Security	Disable SNMP where unnecessary; otherwise restrict access and replace default community strings
h.	Account Review	Audit all router accounts and remove unknown, inactive or unnecessary administrative users
i.	Configuration Review	Examine firewall rules, routing tables, NAT rules, scripts and scheduled tasks for unauthorized modifications
j.	Monitoring	Review authentication, configuration-change and network-traffic logs for indicators of compromise
k.	Compromise Response	If compromise is suspected, isolate the affected router and conduct a full configuration and credential review before restoring service

7. ACTION SUMMARY & RESPONSE PRIORITIES

Sr. No.	Action Type	Specific Steps
a.	RouterOS Patching	Upgrade vulnerable and legacy routers to the latest secure vendor-supported release
b.	Management Exposure	Restrict public access to Winbox, WebFig, SSH and REST API
c.	Password Security	Replace default and weak credentials with strong unique passwords
d.	SNMP Security	Disable unnecessary SNMP and remove default community strings
e.	Account Review	Remove unknown and unnecessary administrative accounts
f.	Configuration Integrity	Review firewall, routing, NAT and scripting configurations
g.	Logging & Monitoring	Monitor authentication attempts and configuration changes
h.	Incident Response	Isolate and investigate routers showing signs of compromise

National Cyber Emergency Response Team (NCERT)

Government of Pakistan

Pak Secretariat, I Block, Islamabad, Pakistan

+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk



National Cyber Emergency Response Team

Government of Pakistan



8. MONITORING & DETECTION REQUIREMENTS

#	Monitoring Activity
1	Monitor repeated failed authentication attempts against Winbox, SSH and WebFig
2	Detect successful administrative logins from unusual or unauthorized source IP addresses
3	Monitor creation or modification of router user accounts
4	Review changes to firewall, NAT and routing configurations
5	Monitor unauthorized or suspicious RouterOS scripts and scheduled tasks
6	Detect unexpected outbound traffic or unusual proxying activity
7	Monitor exposure of management services on internet-facing interfaces
8	Review SNMP access attempts and default community-string usage

National Cyber Emergency Response Team (NCERT)

Government of Pakistan

Pak Secretariat, I Block, Islamabad, Pakistan

+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk