



PUBLIC ANNOUNCEMENT

Malawi CERT Alerts the Public to Critical Vulnerabilities in MikroTik Routers

The Malawi Communications Regulatory Authority (MACRA), through the Malawi Computer Emergency Response Team (Malawi CERT), is alerting the public to known critical vulnerabilities in MikroTik Routers.

Malawi CERT is urging individuals, businesses, organisations, and Internet Service Providers (ISPs) using MikroTik routers to take immediate action, following reports of active exploitation worldwide.

The vulnerabilities, collectively referred to as "**MikroTrick**," are being exploited by cybercriminals to gain unauthorised control of affected MikroTik routers.

What You Should Do

Malawi CERT strongly advises all MikroTik users to:

1. **Update RouterOS immediately** to the latest stable, security-patched version applicable to your device.
2. **Apply the update without delay** if you have access to the router's administration interface.
3. **Contact your ISP or IT service provider** to request an update if you do not manage the router yourself.

Reporting and Assistance

Members of the public and organisations requiring assistance or wishing to report a suspected cybersecurity incident are encouraged to contact Malawi CERT through the following official channels:

- **Portal:** www.mwcert.mw
- **Email:** reporting@mwcert.mw
- **Toll-free:** 261

8th September 2026

Mayamiko Nkoloma, PhD

DIRECTOR GENERAL