

PRODUCT SECURITY NOTIFICATION

Critical PHP vulnerabilities – M!DGE2 cellular routers

Dear valued customers,

We would like to inform you about recently disclosed **critical security vulnerabilities in PHP** (CVE-2026-109618 and CVE-2026-109619), **which affect M!DGE2 legacy cellular routers**.

RACOM has assessed the impact on its product portfolio and provides the following information and recommendations to help customers maintain the security of their networks.

Affected products

The vulnerabilities affect **M!DGE2 legacy cellular routers**, including the latest RACOM firmware version 4.8.40.101, as well as their **predecessors M!DGE, MG102i and MG102**.

These products use the NetModule software platform (NRSW), which incorporates PHP. Under certain conditions, the reported vulnerabilities may allow an unauthenticated attacker to execute malicious code on an affected device through its web services.

Other RACOM products, including RipEX radio modems, M!DGE3 cellular routers, RAY microwave links and WaSP embedded radios, **do not use PHP and are not affected by these vulnerabilities**.

Customer impact and recommended action

The actual exposure depends on the network configuration, particularly the accessibility of the device's web management interface.

RACOM recommends disabling the HTTP/HTTPS web management interface on affected devices. Where this is not operationally feasible, access should be restricted to trusted management hosts only.

Devices operating within private APN networks are generally not directly exposed to the public Internet. Nevertheless, access from other devices within the same network or interconnected networks must also be considered. Appropriate access restrictions and network segmentation remain important.

These measures significantly reduce the potential exposure but do not eliminate the underlying software vulnerabilities.

Kindly follow the technical guidance attached to this document.

Product lifecycle and support

The legacy M!DGE2 router was originally introduced in 2018 and available for standard deliveries until 2023. M!DGE2 was officially declared end-of-life (EOL) in June 2024.

As an EOL product, M!DGE2 is no longer under active software development, and no further firmware updates are planned.

Existing warranty conditions arrangements remain unchanged, despite the M!DGE2 EOL notification.

Since 2023, for new deployments, RACOM recommends M!DGE3, our latest industrial cellular router, offering advanced networking capabilities, modern cybersecurity features and ongoing software development.

Customer support

RACOM remains committed to supporting customers in maintaining reliable communications and planning the long-term continuity of their networks.

For further information please contact us at racom@racom.eu.

Sincerely,

David Marek
Sales Director, RACOM

Technical guidance

Before applying the recommended changes

Customers should back up their device configuration, verify alternative management access and identify any systems that depend on web-based administration.

For remotely deployed devices, configuration changes should preferably be performed during a planned maintenance window. Incorrect access settings may prevent remote administration and require local intervention.

1. Disable the web management interface (recommended)

Before disabling the web interface, ensure that SSH access is enabled and functioning, allowing subsequent administration of the device.

In the Web Manager, navigate to SERVICES → SSH/Telnet Server and enable the SSH server. Verify that the administrative account has CLI shell access and that you can establish an SSH connection.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | **SERVICES** | SYSTEM | LOGOUT

SDK
Administration
Job Management
Testing
DHCP Server
DNS Server
NTP Server
Dynamic DNS
E-mail
Events
SMS
SSH/Telnet Server
SNMP Agent
Let's Encrypt

Telnet Server Configuration

Administrative status: ☐ enabled ☒ disabled
Server port:

SSH Server Configuration

Administrative status: ☒ enabled ☐ disabled
Server port:
Disable admin login: ☐
Disable password-based login: ☐ [upload authorized keys](#)

Apply

For additional security, RACOM recommends restricting SSH access to trusted management hosts and using SSH key-based authentication where practical.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | **SYSTEM** | LOGOUT

System
Settings
Time & Region
Reboot
Authentication
User Accounts
Remote Authentication
Software Update
Software Update
Modem Firmware Update
Software Profiles
Configuration
File Configuration
Factory Configuration
Troubleshooting
Network Debugging
System Debugging
Tech Support
Keys & Certificates

Keys & Certificates
Configuration

Name	Description	Status
Root CA	The root authority used for issuing local certificates	installed
Web Server	The SSL certificates used by the Web server	installed
MQTT Broker	The SSL certificates used by the MQTT broker	missing
SSH Server	The host keys used by the SSH server	installed
SSH Authorization	The keys used for SSH authorization	installed
SSH 'zabbix'	The keys used for SSH authorization of the user 'zabbix'	missing
Authorities	Other certificate authorities which we trust	missing

Erase

It is suggested to change the default SSH port from 22 to user-customized.

For even higher security, it is possible to disable “password-based login” - upload authorized keys by clicking the respective button and follow the procedure.

Login with the same credentials as for the web interface access. Make sure your user has the CLI shell access, at least.

System

Settings

Time & Region

Reboot

Authentication

User Accounts

Remote Authentication

Software Update

Software Update

Modem Firmware Update

Software Profiles

Configuration

File Configuration

Factory Configuration

Troubleshooting

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | **SYSTEM** | LOGOUT

Edit Administrator Account

Username: admin

Description: Administrator

Shell: CLI

Store password unencrypted: enable

Allow CLI-PHP: allow

Old password: show

New password: show

Confirm new password: show

Apply

Connect to the device through SSH using an account with sufficient privileges and execute the following commands:

- `cli-set http.status=0`
- `cli-set https.status=0`

These commands disable HTTP and HTTPS web management.

Operational consequences: Disabling the web interface removes access to browser-based configuration, monitoring and maintenance functions. It may also affect external management applications or automation tools that depend on HTTP/HTTPS services, including CLI-PHP.

Normal routing, VPN connections and data communications are not expected to be affected. However, customers should verify any application-specific dependencies before proceeding. Administration remains available through SSH (CLI), if access has been configured and verified beforehand.

Restoring web management access: If browser-based administration is required later, the relevant services can be temporarily re-enabled through SSH using:

- `cli-set http.status=1`
- `cli-set https.status=1`

Enable only the services required, preferably HTTPS, and ensure access is restricted to trusted management hosts. Once the configuration changes are completed, disable the web interface again.

2. Restrict web management access (alternative)

Where disabling the web interface is not operationally feasible, its accessibility should be carefully restricted.

For devices operating within a private APN, verify that the network is isolated as intended and that web management cannot be accessed from unauthorized devices or interconnected networks.

For devices using a public APN, particular attention should be paid to whether the device has a publicly reachable IP address. Private addresses may reduce direct Internet exposure, but do not necessarily prevent access through other network paths.

RACOM recommends:

- *Using secure management connections, such as IPsec or OpenVPN tunnels, and ensuring that web management is not independently accessible from untrusted networks.*
- *Configuring firewall rules under the FIREWALL menu to permit HTTP/HTTPS access only from explicitly authorized management addresses.*
- *Reviewing access restrictions across all relevant interfaces and connected networks.*
- *Disabling HTTP-based CLI-PHP access unless it is specifically required.*

For additional information, please refer to the [M!DGE2 User Manual](#).

For assistance with the recommended configuration changes, please contact RACOM Technical Support at support@racom.eu.