RFCODE

June 1st, 2026

CVE-2026-42945

Summary

The M250 is not affected by CVE-2026-42945, a heap overflow vulnerability in the NGINX HTTP rewrite module (ngx_http_rewrite_module). The vulnerable module is not present in the NGINX build shipped on the M250 firmware. No customer action is required to mitigate this CVE on the M250.

Vulnerability scanners that match purely on the reported NGINX version banner will flag the device as potentially affected, because the version string falls within the range listed in the CVE. This is a false positive in the M250 context: the affected module has been removed from the build and the conditions required for exploitation cannot be created on the device.

1. Purpose of the NGINX Service

NGINX is used solely as a lightweight web server to host the device's local configuration interface and status pages. This enables direct device configuration and limited data visibility without requiring the full CenterScape software stack.

2. Accessibility

The HTTPS service on port 443 is intended for local access (for example, provisioning and configuration). It can be enabled or disabled via device settings, and it is typically restricted to trusted networks or controlled via external network policies.

3. CVE-2026-42945 Applicability Assessment

The referenced vulnerability is a heap overflow in the NGINX HTTP rewrite module. It applies specifically to deployments where NGINX is:

- Built with the HTTP rewrite module (ngx_http_rewrite_module) included, and
- Configured to use rewrite module directives such as rewrite, if, set, return, or break to process attacker influenced input.

On the M250, these conditions are not met for the following reasons:

- The NGINX build used in the firmware is compiled with --without-http_rewrite_module, which removes the vulnerable module from the binary.

- As a result, NGINX does not support rewrite, if, set, return, break, or any other directive provided by the HTTP rewrite module.
- The vulnerable code path described in the CVE is therefore not present in the M250 firmware and cannot be reached at runtime, regardless of configuration or input.

4. Technical Detail for Security Teams

Why the rewrite module matters

CVE-2026-42945 is exploitable only along a code path inside the NGINX HTTP rewrite module. If the module is not compiled into the binary, the vulnerable code is not loaded, not executable, and not reachable by any request. There is no configuration that can re□enable it at runtime.

Build-time exclusion

The M250 firmware compiles NGINX with --without-http_rewrite_module. Configuration directives provided by that module (including rewrite, if, set, return, and break) are not recognized by the build and cannot be enabled. Any configuration file referencing them would fail to load.

Runtime behavior

At runtime, NGINX on the M250 serves only the local configuration UI and status pages. Request handling does not pass through the rewrite module because the module is not present in the binary, so the heap□overflow code path identified by CVE-2026-42945 is unreachable.

Why version-based scanners may still flag the M250

Vulnerability scanners that match purely on the reported NGINX version banner will flag the device as potentially affected, because the version string falls within the range listed in the CVE. This is a false positive in the M250 context: the affected module has been removed from the build and the conditions required for exploitation cannot be created on the device.

Conclusion

Because the NGINX HTTP rewrite module is not present in the M250 build, the vulnerable code path described in CVE-2026-42945 cannot be reached. The M250 is therefore not affected by this vulnerability, despite the detected NGINX version.

Customers do not need to take any action on the M250 to mitigate CVE-2026-42945. We recommend continuing to follow standard practice of restricting access to the local configuration interface to trusted networks.