RFCODE

May 1st, 2026

CVE-2026-1642

Summary

The M250 is not affected by CVE-2026-1642. The vulnerability requires NGINX to be configured to proxy traffic to an upstream HTTPS server, which the M250 firmware does not do. The NGINX build shipped on the M250 is compiled without the HTTP proxy module, so it cannot perform the proxying behavior the CVE describes. No customer action is required to mitigate this CVE on the M250.

The remainder of this document explains how NGINX is used on the device and provides the technical detail security teams need to confirm this assessment independently.

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 feature 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-2026-1642 Applicability Assessment

The referenced vulnerability applies specifically to deployments where NGINX is:

- Configured to proxy requests to upstream TLS (HTTPS) servers, and
- Operating in a scenario where a man-in-the-middle attacker can interfere with that upstream connection.

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

- The NGINX build used in the firmware is compiled without the HTTP proxy module (--without-http_proxy_module).

- As a result, NGINX does not support proxy_pass or any HTTP/HTTPS upstream proxying functionality.
- The only upstream interaction present is via local inter-process communication using a Unix domain socket (for example, fastcgi_pass unix:/root/echo.sock).
- NGINX does not establish outbound network connections to upstream servers, nor does it proxy traffic to external TLS endpoints.

4. Technical Detail for Security Teams

Why the proxy module matters

CVE-2026-1642 is exploitable only along a code path that exists when NGINX acts as a reverse proxy to an upstream TLS server and an attacker can interpose on that upstream connection. The vulnerable code path is contained within the HTTP proxy module.

Build-time exclusion

The M250 firmware compiles NGINX with --without-http_proxy_module, which removes the proxy module from the binary entirely. Configuration directives such as proxy_pass, proxy_ssl_*, and related upstream TLS settings are not recognized by the build and cannot be enabled at runtime.

Runtime behavior

At runtime, NGINX on the M250 serves only the local configuration UI and status pages. The only “upstream” it speaks to is a local FastCGI handler reached over a Unix domain socket (e.g. fastcgi_pass unix:/root/echo.sock). There is no outbound TCP connection to a remote HTTPS server, and therefore no opportunity for a network-based man-in-the-middle attacker to influence an upstream TLS exchange.

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 feature has been removed from the build and the conditions required for exploitation cannot be created on the device.

Conclusion

Because the required proxying functionality is not present in the NGINX build and no upstream TLS communication occurs, the conditions necessary to exploit CVE-2026-1642 are not present. 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-2026-1642. We recommend continuing to follow standard practice of restricting access to the local configuration interface to trusted networks.