RFCODE

June 1st, 2026

CVE-2024-7347

Summary

The M250 is not affected by CVE-2024-7347, an out-of-bounds read vulnerability in the NGINX MP4 module (ngx_http_mp4_module). The vulnerable module is an optional, opt-in component of NGINX and is not enabled by default. The M250 firmware does not include the build flag required to enable it, so the vulnerable module is not present in the binary. 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 not been compiled into 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-2024-7347 Applicability Assessment

The referenced vulnerability is an out-of-bounds read in the NGINX MP4 module. It applies specifically to deployments where NGINX is:

- Built with the MP4 module (ngx_http_mp4_module) explicitly enabled via --with-http_mp4_module, and
- Configured to use the mp4 directive to serve MP4 media files via pseudo-streaming, where an attacker can supply a crafted MP4 file.

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

- The MP4 module is an optional NGINX module that is not compiled in by default; it must be explicitly enabled at build time with --with-http_mp4_module.

- The M250 firmware build does not include the --with-http_mp4_module flag, so the module is not present in the resulting binary.
- As a result, NGINX on the M250 does not support the mp4 directive or any MP4 pseudo‑streaming functionality, and the vulnerable code path is not present at runtime.

4. Technical Detail for Security Teams

Why the MP4 module matters

CVE-2024-7347 is exploitable only along a code path inside the NGINX MP4 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 (opt-in module)

The MP4 module is not part of NGINX's default build. It is included only when --with-http_mp4_module is passed to configure. The M250 firmware build does not pass this flag, so the module is omitted from the binary. The mp4 directive is therefore unknown to the build and cannot be enabled. Any configuration file referencing it would fail to load.

Runtime behavior

At runtime, NGINX on the M250 serves only the local configuration UI and status pages. There is no MP4 media handling, and request processing never reaches the MP4 module because the module is not present in the binary, so the out-of-bounds read code path identified by CVE-2024-7347 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 not been compiled into the build and the conditions required for exploitation cannot be created on the device.

Conclusion

Because the NGINX MP4 module is not present in the M250 build, the vulnerable code path described in CVE-2024-7347 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-2024-7347. We recommend continuing to follow standard practice of restricting access to the local configuration interface to trusted networks.