SECURITY ADVISORY

Symphony MX web interface missing common security headers in HTTP response

Advisory ID	CSA-2025-61
Title	Symphony MX web interface missing common security headers in HTTP response
Devices	Symphony MX
Severity	Medium
CVSS score	5.3
CVSS base	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N
First published	19.12.2025
Last updated	19.12.2025
Version	1.0

Summary of vulnerability notification

Several vulnerabilities have been discovered in the HTTP server response of the Symphony MX web interface which are caused by missing common HTTP security headers. Due to insufficient cache control, a threat actor could read sensitive data stored within the browser cache on the local machine. The missing content type options header permits the browser to incorrectly identify content types when no content type is specified by the server. A firmware update is required to fix the vulnerability.

Affected products

- Symphony MX below v4.7.1

Software updates

- Symphony MX v4.7.1 or higher

Workaround

There is no workaround for the problem.

Exploitation and public announcements

The Commend Security Board is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

Acknowledgement

This vulnerability was discovered and responsibly disclosed by Dominik Schneider of Amazon Security and Kevin Schaller of Amazon Security.

COMMEND INTERNATIONAL GMBH would like to thank the security researchers for reporting this issue.

Sources

This vulnerability was found during external security penetration testing.

Contact and coordinated disclosure

support@commend.com

COMMEND INTERNATIONAL GMBH
Saalachstraße 51
5020 Salzburg, Austria

Change log

- 22.10.2025 – External finding
- 29.10.2025 – Vulnerability confirmed
- 21.11.2025 – Vulnerability fixed and fix verified
- 19.12.2025 – First published