SECURITY ADVISORY

commend

Symphony MX web interface allows uploading arbitrary data to Media

Advisory ID	CSA-2025-60
Title	Symphony MX web interface allows uploading arbitrary data to Media
Devices	Symphony MX
Severity	Medium
CVSS score	5.3
CVSS base	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/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

A vulnerability has been discovered in the Symphony MX web interface which allows uploading arbitrary data to the internal media storage "Media", where audio and images are stored. Due to insufficient input and file content validation, an authenticated attacker could upload malicious files. If successful, a threat actor can trick an authenticated user to run malicious file content on the local machine. A firmware update is required to fix the vulnerability.

Note: Symphony MX devices cannot protect authenticated users from downloading and executing files.

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
- 27.11.2025 – Vulnerability fixed and fix verified
- 19.12.2025 – First published