# SECURITY ADVISORY

# Symphony MX web interface vulnerable to clickjacking and cross-frame scripting (XFS)

| | |
|---|---|
| **Advisory ID** | CSA-2025-55 |
| **Title** | Symphony MX web interface vulnerable to clickjacking and cross-frame scripting (XFS) |
| **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 Symphony MX web interface. Due to missing HTTP security headers, the web interface is vulnerable to clickjacking and cross-frame scripting (XFS) attacks. An attacker could embed the web interface into a crafted HTML web page. Such a malicious web page could introduce hidden mechanism to steal the credentials during user authentication or to modify the device configuration without being noticed. 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

- 13.02.2025 – First external finding
- 24.02.2025 – Vulnerability confirmed
- 24.02.2025 – Priority decreased to LOW
- 20.10.2025 – Second external finding
- 20.10.2025 – Priority increased to MEDIUM
- 20.10.2025 – Vulnerability fixed and fix verified
- 19.12.2025 – First published