SECURITY ADVISORY

Local privilege escalation via privileged executable

Advisory ID	CSA-2025-58
Title	Local privilege escalation via privileged executable
Devices	Symphony MX
Severity	High
CVSS score	7.3
CVSS base	CVSS:4.0/AV:L/AC:L/AT/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
First published	19.12.2025
Last updated	19.12.2025
Version	1.0

Summary of vulnerability notification

The Symphony MX device contains a privileged executable file that is writeable, creating a critical security vulnerability. Threat actors with access to the device could exploit this vulnerability by modifying the executable with malicious code, which could then be executed with root privileges. If successful, attackers could achieve complete system compromise, establish persistence, execute arbitrary commands with root privileges or create backdoors for ongoing unauthorised access. A firmware update is required to fix the vulnerability.

Note: Symphony MX devices are protected against local attack vectors, as remote maintenance via SSH is disabled by default.

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
- 10.12.2025 – Vulnerability fixed and fix verified
- 19.12.2025 – First published