SECURITY ADVISORY

Local privilege escalation via service hijacking

Advisory ID	CSA-2025-56
Title	Local privilege escalation via service hijacking
Devices	VirtuoSIS, S3 and S6
Severity	Critical
CVSS score	9.3
CVSS base	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:H/SA:H
First published	17.12.2025
Last updated	17.12.2025
Version	1.0

Summary of vulnerability notification

A security issue was discovered where local users can escalate privileges by manipulating environment variables that affect privileged processes. Threat actors could exploit this vulnerability by injecting malicious values into environment variables used by services running with elevated privileges. If successful, attackers could execute arbitrary commands with elevated privileges, potentially leading to complete system compromise, unauthorised access to sensitive data or the ability to modify the system configuration or security controls.

Affected products

- VirtuoSIS, S3 and S6 below v15.3.0

Software updates

- VirtuoSIS_15.3.0.ova or higher
- VirtuoSIS_15.3.0.vsu or higher
- VirtuoSIS_15.3.0.zip 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
- 27.10.2025 – Vulnerability confirmed
- 26.11.2025 – Vulnerability fixed and fix verified
- 17.12.2025 – First published