SECURITY ADVISORY

Vulnerabilities have been discovered in the SIP engine

Advisory ID	CSA-2024-48
Title	Vulnerabilities have been discovered in the SIP engine
Devices	VirtuoSIS, S3 and S6
Severity	Medium
CVSS score	6.5
CVSS base	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
First published	03.05.2024
Last updated	03.05.2024
Version	1.0

Summary of vulnerability notification

Several vulnerabilities have been discovered in the SIP engine. VirtuoSIS is missing a security-related update.
A SIP engine package upgrade has been carried out and new VirtuoSIS templates are available for download.

The update for S3 and S6 must be carried out via VirtuoBRO using the system reset feature or via the command line via the command "cis-ctl system-reset" by using the updated *.vsu file.
The update for VirtuoSIS in virtual environments must be carried out via the deployment of the updated *.ova or *.zip template.
Consider creating a backup for any recovery purposes. For more details on the update process, please refer to the VirtuoSIS setup guide available at https://clibrary-online.commend.com/

We recommend carrying out the update in accordance with your IT policy.

Affected products

- VirtuoSIS, S3 and S6 below v14.0.1

Software updates

- VirtuoSIS_14.0.1.ova or higher
- VirtuoSIS_14.0.1.vsu or higher
- VirtuoSIS_14.0.1.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

-

Sources

This vulnerability was found during external security penetration testing.

This vulnerability is dealt with at

https://nvd.nist.gov/vuln/detail/CVE-2020-28242

https://nvd.nist.gov/vuln/detail/CVE-2020-28327

Contact and coordinated disclosure

support@commend.com

COMMEND INTERNATIONAL GMBH
Saalachstraße 51
5020 Salzburg, Austria

Change log

- 08.04.2022 – External finding
- 08.04.2022 – Vulnerability confirmed
- 08.02.2024 – Vulnerability fixed and fix verified
- 03.05.2024 – First published