NATIONAL CSIRT CY

CVE-2025-34028

28/04/2025

Vulnerability in Commvault Command Center allows RCE

CONFIDENTIAL

The content of this document is intended solely for use by the natural or legal person to whom it is addressed. If you gain access to this document by mistake, you should be aware that any forwarding, copying or disclosure of its content to any other person is strictly prohibited, and you must inform the sender immediately.

Executive Summary

A threat researcher named Sonny Macdonald discovered a path traversal vulnerability in Commvault Command Center that allows remote code execution.

This is a vulnerability with a CVSS Score 9.0/10.

Proof of concept of the exploit can be found here: https://github.com/watchtowrlabs/watchTowr-vs-Commvault-PreAuth-RCE-CVE-2025-34028

Affected versions and mitigation

The specific vulnerability affects only the 11.38 release.

Affected versions are from 11.38.0 to 11.38.19 both in Windows and Linux

Commvault pushes automatically the updates without the need for manual intervention. However, Commvault said that if it’s not possible to install the update the Command Center should be isolated from external network access.

Common Vulnerabilities & Exposures

https://nvd.nist.gov/vuln/detail/CVE-2025-34028

Common Weakness Enumeration

https://cwe.mitre.org/data/definitions/22.html

Please distribute this information among your subsidiaries and partners, and also share with us any pertinent information and findings you may have (e.g IOCs, TTPs etc)

The Digital Security Authority extends its appreciation for the continued collaboration.

Disclaimer

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.