# CVE Detail – CVE-2024-5565

The Vanna library uses a prompt function to present the user with visualized results, it is possible to alter the prompt using prompt injection and run arbitrary Python code instead of the intended visualization code. Specifically - allowing external input to the library’s “ask” method with "visualize" set to True (default behavior) leads to remote code execution.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.87899

## CVSS Scoring

CVSS v3.1 Score: 8.1

Severity: HIGH

## Mapped CWE(s)

* CWE-94: Improper Control of Generation of Code ('Code Injection')

## CAPEC(s)

* CAPEC-242: Code Injection
* CAPEC-35: Leverage Executable Code in Non-Executable Files
* CAPEC-77: Manipulating User-Controlled Variables

## ATT&CK Techniques

* T1027.009: Embedded Payloads
* T1564.009: Resource Forking
* T1027.006: HTML Smuggling

## Used By (Actors/Tools)

* Pikabot (malware)
* macOS.OSAMiner (malware)
* EnvyScout (malware)
* Emotet (malware)
* DUSTTRAP (malware)
* BADHATCH (malware)
* DUSTPAN (malware)
* Moneybird (malware)
* Keydnap (malware)
* IcedID (malware)
* CHIMNEYSWEEP (malware)
* MultiLayer Wiper (malware)
* Netwalker (malware)
* SMOKEDHAM (malware)
* Uroburos (malware)
* DEADEYE (malware)
* ComRAT (malware)
* QakBot (malware)
* OSX/Shlayer (malware)
* DEADWOOD (malware)
* Dtrack (malware)
* Invoke-PSImage (tool)
* Lazarus Group (intrusion-set)
* TA577 (intrusion-set)
* APT29 (intrusion-set)
* C0021 (campaign)
* Moonstone Sleet (intrusion-set)