Forensic Investigation Report

Case Information

Challenge Name: Clematis

Investigation Type: DFIR Challenge

Initial Discovery

While going through the system, I found multiple folders inside `C:\Users\Mizi\Music`. Since this was a Windows 10 VM, I used PowerShell to enumerate files and look for anything suspicious.

During this search when I typed in `ps`, a file named `31.jpg.ps1` was discovered. This immediately stood out as a classic double-extension trick where Windows hides the real extension and makes the file look like an image.

Repository Analysis

The file was located inside `C:\Users\Mizi\Music\WorldCollapsing`, which turned out to be a cloned Git repository. To understand how the file got there,i looked at the `HEADS` file present in `C:\Users\Users\Mizi\Music\WorldCollapsing\.git\logs`.

This gave me

```
0000000000000000000000000000000000000000
976e900f0e904085bbce393bec3b7b63a41a4062 Mizi <mizi@vivimenginc.com>
1765354698 -0800 commit (initial): initial commit!!

976e900f0e904085bbce393bec3b7b63a41a4062
6afb28994515f7f61030e5d556b608e79e36b16c Luka <luka@heperu.com>
1765357212 -0800 commit: add images :3

6afb28994515f7f61030e5d556b608e79e36b16c
be43f602419301ab1feb28af289c3fc5ddfaf3a8 Mizi <mizi@vivimenginc.com>
1765457273 -0800 commit: add images :3

be43f602419301ab1feb28af289c3fc5ddfaf3a8
378ef2dc98ed416cbf837181d1961df25e44eb09 Mizi <mizi@vivimenginc.com>
1765457273 -0800 commit: more images added :3

378ef2dc98ed416cbf837181d1961df25e44eb09
f89b55297a9b9281505f27e36ece1e5150836699 Mizi <mizi@vivimenginc.com>
1765457274 -0800 commit: batch of images :3
```

```
f89b55297a9b9281505f27e36ece1e5150836699
33464523277fcff11508c18faa86ddb15184c364 Mizi <mizi@vivimenginc.com>
1765457275 -0800 commit: add images :3

33464523277fcff11508c18faa86ddb15184c364
b762db10a552bb05f3c292607b51c8fca10fbc13 Mizi <mizi@vivimenginc.com>
17543933275 -0800filter-branch: rewrite
```

Malicious Commit Identification

Among all the commits, only one commit was authored by a user named `Luka`, which made it stand out. Running `git show --name-status` on this commit showed that a new file `images/31.jpg.ps1` was added and the `.cursor/mcp.json` file was modified.

The change to `mcp.json` caused the malicious PowerShell file to be executed, confirming this commit as the point where the system was compromised.

Exploit Identification

Based on the behavior observed, the exploit matched an MCPoison, which is tracked as **`CVE-2025-54136`**.

Recovering the Original Commit

Further inspection showed that `git filter-branch` had been used, meaning the visible commit ID i.e. `6afb28994515f7f61030e5d556b608e79e36b16c`, was not the original one. To recover the real commit, `git blame` was run on `31.jpg.ps1`, which revealed a shortened commit hash i.e `c0df0ebe`

Running `git rev-parse` on this shortened hash returned the full original commit ID:

`c0df0ebeb988e991418029e3021fb7f8542068b2`

Conclusion

In conclusion, the attacker exploited CVE-2025-54136 to gain code execution through a poisoned MCP configuration. They introduced a malicious PowerShell script disguised as an image file and attempted to hide their activity by rewriting Git history. All required artifacts for the challenge were successfully identified.

Final Flag

nite{CVE-2025-54136_c0df0ebeb988e991418029e3021fb7f8542068b2_31.jpg.ps1}