Establish procedures to investigate and verify unfamiliar or unexpected commit authors before incorporating changes

5. **CODE SIGNING REQUIREMENTS:**

   Implement mandatory code signing for repository commits from trusted, verified developers

6. **SANDBOXING IMPLEMENTATION:**

   Require IDE-executed commands to operate within restricted sandboxed environments

7. **SECURITY AWARENESS TRAINING:**

   Educate development personnel on supply-chain attack vectors targeting developer tooling

11. RECOVERED EVIDENCE

The investigation successfully recovered the following forensic evidence flag, which encodes the key components of the attack methodology:

```
nite{CVE-2025-54135/6_c0df0ebeb988e991418029e3021fb7f8542068b2_31.jpg.ps1}
```

EVIDENCE FLAG COMPONENT ANALYSIS:

- **CVE-2025-54135/6:**

  Identified vulnerability CVE identifiers documenting the MCP configuration poisoning vulnerability

- **C0DF0EBEB988E991418029E3021FB7F8542068B2:**

  Git commit hash of the malicious commit introducing the exploit configuration

- **31.JPG.PS1:**

  Filename of the payload file containing the obfuscated PowerShell script

END OF REPORT

Document Classification: Investigation Complete

Report Generated: January 2025

Challenge Designation: Incident Response 1 - WorldCollapsing Case

Investigation Status: CLOSED