CVE-2024-51378 Research Assignment

- **Basic Information**
    - CVE ID: **51378**
    - Name of Vulnerability: **CyberPanel Incorrect Default Permissions Vulnerability**
    - Affected Software/Application: **CyberPanel**
    - Affected Versions: **All versions up to and including 2.3.7**
- **Vulnerability Details**
    - Type of Vulnerability (e.g., command injection, buffer overflow): **command injection**
    - Description of Vulnerability: **getresetstatus in dns/views.py and ftp/views.py in CyberPanel (aka Cyber Panel) before 1c0c6cb allows remote attackers to bypass authentication and execute arbitrary commands via /dns/getresetstatus or /ftp/getresetstatus by bypassing secMiddleware (which is only for a POST request) and using shell metacharacters in the statusfile property, as exploited in the wild in October 2024 by PSAUX. Versions through 2.3.6 and (unpatched) 2.3.7 are affected.**
    - Vulnerable Components: **getresetstatus in dns/views.py and ftp/views.py**
- **Impact**
    - Potential Impact on Affected Systems: **Gain Privileges or Assume Identity; Bypass Protection Mechanism**
    - Access Level Achievable by Attacker: **root-level**
    - Known Real-World Exploits (if applicable):
- **Exploitation**
    - Attack Vector (e.g., network, local, physical): **Network**
    - Steps to Exploit the Vulnerability:

        1. Initial Testing

        2. Analyzing the Security Middleware

        3. The Bypass Discovery

        4. Triggering the Vulnerability

    - Available Proof of Concept (PoC):

https://github.com/refr4g/CVE-2024-51378

- Active Exploitation in the Wild (Yes/No): **Yes**

- **Mitigation and Remediation**
  - Patches Available: https://github.com/usmannasir/cyberpanel/commit/1c0c6cbcf71abe573da0b5fddfb9603e7477f683
  - Workarounds: **Decryption tool:** https://gist.github.com/gboddin/d78823245b518edd54bfc2301c5f8882#file-0-decrypt-sh
  - Steps to Mitigate the Risk: According to Cyberpanel's instructions:

There are two scenarios: one for users with SSH access and one for users without it.

1. If You Have SSH Access:

Simply update your panel using our update guide. No further action is needed.

2. If You Don't Have SSH Access:

to block IP or port 22 access. Contact your provider and request they enable port 22. Once they do, update the panel and, if needed, share access with our support team at

  - Recommendations for System Administrators: **Conduct a system wide version upgrade**

- **Technical Analysis**
  - Code Review of Affected Components (if available):

"dns/views.py":

```
userID = request.session['userID']

currentACL = ACLManager.loadedACL(userID)

if currentACL['admin'] == 1:
```

```
            pass
        else:
            return ACLManager.loadErrorJson('FilemanagerAdmin', 0)
```

"ftp/views.py":

```
userID = request.session['userID']

currentACL = ACLManager.loadedACL(userID)

if currentACL['admin'] == 1:
    pass
else:
    return ACLManager.loadErrorJson('FilemanagerAdmin', 0)
```

- How the Vulnerability Could Have Been Prevented: **Vulnerability detection prior to releasing the affected versions**
- Relevant Secure Coding Practices: **Not only do vulnerability Analysis but also have a human read each possible vulnerable section of code**

- **Security Lessons Learned**
  - Root Cause of the Vulnerability: **Improper Coding**
  - Importance of Patch Management: **Prevent future cyberattacks**
  - Similar Historical Vulnerabilities: **CVE-2024-51567**
- **References**
  - Official Advisory Links:

    https://cwe.mitre.org/data/definitions/78.html

    https://cwe.mitre.org/data/definitions/420.html

    https://cyberpanel.net/KnowledgeBase/home/change-logs/

https://cyberpanel.net/blog/detials-and-fix-of-recent-security-issue-and-patch-of-cyberpanel

- Related Articles and Blogs:
  https://www.bleepingcomputer.com/news/security/massive-psaux-ransomware-attack-targets-22-000-cyberpanel-instances/
- Proof of Concept Repositories: https://github.com/refr4g/CVE-2024-51378
  https://refr4g.github.io/posts/cyberpanel-command-injection-vulnerability/
- Tools to Test or Detect the Vulnerability:

  Decryption Tool:
  https://gist.github.com/gboddin/d78823245b518edd54bfc2301c5f8882#file-0-decrypt-sh