مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical RCE Vulnerabilities in CyberPanel

Tracking #:432316454

Date:30-10-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed three critical remote code execution (RCE) vulnerabilities in CyberPanel are currently under active exploitation by PSAUX Ransomware.

TECHNICAL DETAILS:

Three critical remote code execution (RCE) vulnerabilities in CyberPanel versions 2.3.5,2.3.6 and 2.3.7, tracked as CVE-2024-51567, CVE-2024-51568, and CVE-2024-51378, are currently under active exploitation. These vulnerabilities allow unauthenticated attackers to gain root access, enabling complete control over compromised servers.

Vulnerabilities Identified:

1. **CVE-2024-51567**:
   - upgrademysqlstatus in databases/views.py in CyberPanel (aka Cyber Panel) before 5b08cd6 allows remote attackers to bypass authentication and execute arbitrary commands via /dataBases/upgrademysqlstatus 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.
   - **CVSS Score**: 10,Critical

2. **CVE-2024-51568**:
   - **Description**: CyberPanel (aka Cyber Panel) before 2.3.5 allows Command Injection via completePath in the ProcessUtilities.outputExecutioner() sink. There is /filemanager/upload (aka File Manager upload) unauthenticated remote code execution via shell metacharacters.
   - **CVSS Score**: 10, Critical

3. **CVE-2024-51378**:
   - 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**.**
   - **CVSS Score**: 10, Critical

Impact Assessment

- **Scale of Exposure**: As of October 26, over 21,761 vulnerable CyberPanel instances were online, managing more than 152,000 domains and databases.
- **Ransomware Deployment**: The PSAUX ransomware, identified in June 2024, utilizes these vulnerabilities to:
  - **Encrypt Data**: Use unique AES keys for file encryption.
  - **Create Ransom Notes**: Generate index.html files in directories and display ransom notes in the /etc/motd.
  - **Encrypt Keys**: Encrypt AES keys and Initialization Vectors with an embedded RSA key

RECOMMENDATIONS:

- Users must update their CyberPanel installations to the latest patched versions immediately.
- Regularly back up all critical data stored on CyberPanel instances to facilitate recovery in case of ransomware infection or other incidents.
- Decryptor Available: Security Researchers released a decryptor for files encrypted in this campaign. However, caution is advised when using it.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

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