مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Critical Vulnerability in CyberPanel

Tracking #:432316645

Date:18-12-2024

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in CyberPanel that could potentially be exploited to gain full control over affected systems.

## TECHNICAL DETAILS:

A critical vulnerability (CVE-2024-53376) exists in CyberPanel, a widely-used web hosting control panel. The flaw, present in versions prior to 2.3.8, allows authenticated users to inject and execute operating system (OS) commands, leading to full system compromise. This vulnerability is triggered by a crafted HTTP OPTIONS request to the /websites/submitWebsiteCreation endpoint, which bypasses security mechanisms and grants attackers unauthorized access to the underlying server OS.

**Vulnerability Details:**

- **CVE-2024-53376**
- Attack vector: Authenticated access to the CyberPanel web interface
- Exploitation method: HTTP OPTIONS request to the vulnerable endpoint
- The vulnerability allows attackers to inject shell metacharacters into the phpSelection field, bypassing security measures and executing arbitrary commands with root-level permissions.
- A Proof-of-Concept (PoC) is available on GitHub, demonstrating the exploit's simplicity and potential for system compromise
- Successful exploitation of this vulnerability can lead to:
    - **Achieve root-level access**: Exploiters can execute commands with root privileges, gaining full control over the server.
    - **Exfiltrate sensitive data**: If the CyberPanel installation folder is accessible, attackers can extract sensitive data stored on the server.
    - **Compromise infrastructure**: Web hosting servers running vulnerable CyberPanel versions can become entry points for further attacks, jeopardizing hosted websites and customer data.

**Affected Versions:**

- CyberPanel versions prior to 2.3.8

**Fixed Versions:**

- CyberPanel 2.3.8 or later

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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://nvd.nist.gov/vuln/detail/CVE-2024-53376