مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Actively Exploited Vulnerability in CWP (Control Web Panel)

Tracking #:432317942

Date:05-11-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

ADVISORY

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Control Web Panel (CWP), formerly CentOS Web Panel that allows remote attackers to execute arbitrary commands on affected servers without authentication.

TECHNICAL DETAILS:

A critical remote code execution vulnerability (CVE-2025-48703, CVSS 9.0) has been discovered in Control Web Panel (CWP), formerly CentOS Web Panel. The flaw allows unauthenticated attackers to execute arbitrary commands on the server through the file manager interface due to improper authentication checks and unsanitized input validation. Exploitation can lead to complete compromise of affected systems.

Vulnerability Details

- **CVE-2025-48703**
- Severity: Critical (CVSS 9.0)
- The vulnerability exists in the handling of the t_total parameter within the filemanager changePerm request. CWP fails to properly sanitize user input and does not sufficiently enforce authentication checks on this endpoint.
- Attackers can send crafted HTTP POST requests directly to the file management endpoint, typically accessible on port 2083.
- By injecting shell metacharacters into the t_total parameter (originally intended to specify numeric file permissions), adversaries can trigger arbitrary command execution.
- Successful exploitation allows remote code execution under the privileges of the specified non-root user, which can be leveraged to establish a reverse shell or exfiltrate sensitive data.

Affected Versions

- CWP versions prior to 0.9.8.1205

Fixed Versions

- CWP version 0.9.8.1205 and later

RECOMMENDATIONS:

- Update immediately to CWP version 0.9.8.1205 or newer.
- Limit administrative interface access (port 2083) to internal or trusted IP addresses only.
- Deploy a web application firewall (WAF) capable of detecting and blocking malicious payloads containing shell metacharacters.
- Review server and application logs for unusual filemanager or permission change requests.
- Perform post-upgrade security auditing and integrity verification to ensure the environment has not been compromised.

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-2025-48703