مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical Remote Code Execution Vulnerability in Convoy

Tracking #:432317408

Date:24-06-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability has been discovered in Convoy, a modern KVM server management panel widely used by hosting providers.

TECHNICAL DETAILS:

A critical vulnerability has been discovered in Convoy, a modern KVM server management panel widely used by hosting providers. Tracked as CVE-2025-52562, the flaw allows unauthenticated remote code execution (RCE) via specially crafted HTTP requests. It affects all Convoy versions from 3.9.0-rc.3 through 4.4.0.

The root cause lies in the LocaleController, which fails to properly sanitize locale and namespace parameters, enabling directory traversal and arbitrary PHP file inclusion. This vulnerability has been assigned a CVSS score of 10.0, the highest possible rating.

Successful exploitation can lead to full remote code execution, data theft, and complete server compromise. Immediate patching or mitigation is strongly advised.

Vulnerability Details:

- CVE ID: CVE-2025-52562
- Severity: Critical (CVSS 10.0)
- Impact: Unauthenticated Remote Code Execution
- Affected Product: Convoy KVM Server Management Panel
- Affected Versions: 3.9.0-rc.3 through 4.4.0
- Fixed Version: 4.4.1 and later
- Exploit Status: No public exploit disclosed; proof-of-concept likely feasible
- Attack Vector: Remote (via HTTP request using locale and namespace parameters)
- Root Cause: Directory traversal and unsafe file inclusion in LocaleController

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade Convoy to fixed version or later, which contains the official patch.

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://github.com/ConvoyPanel/panel/security/advisories/GHSA-43g3-qpwq-hfgg