



مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



Actively Exploited Vulnerability in Wing FTP Server  
Tracking #:432318617  
Date:17-03-2026

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 INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a security vulnerability in Wing FTP Server that is actively being exploited. This flaw allows access to sensitive internal system information, potentially enabling further exploitation and deeper compromise of affected systems.

## TECHNICAL DETAILS:

A vulnerability has been identified in Wing FTP Server that is actively being exploited by malicious actors. The flaw allows authenticated attackers to disclose sensitive internal server path information, which can be leveraged to facilitate further attacks and deeper system compromise.

### Vulnerability Details

- **CVE ID:** CVE-2025-47813
- **Severity:** Medium **CVSS Score:** 4.3
- **Vulnerability Type:** Information Disclosure
- The vulnerability resides in the /loginok.html endpoint of Wing FTP Server and is caused by improper validation of the length of the UID session cookie. An authenticated attacker can exploit this issue by sending a crafted POST request containing an excessively long UID value, which exceeds the maximum path size supported by the underlying operating system. This triggers an error response that discloses the full local file system path of the application. The exposed path information can be used by attackers to map internal directories, identify sensitive file locations, and support further exploitation, including chaining with other vulnerabilities such as CVE-2025-47812.

### Affected Versions

- Wing FTP Server versions prior to 7.4.4

### Fixed Versions

- Wing FTP Server version 7.4.4 or later

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Wing FTP.

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-2025-47813>