مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Critical Vulnerability in Wing FTP Server

Tracking #:432317481
Date:14-07-2025

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

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a critical severity vulnerability in Wing FTP Server is under active exploitation, allowing remote attackers to execute arbitrary system commands via the web interface.

TECHNICAL DETAILS:

This vulnerability arises from improper handling of null (\0) bytes in the Wing FTP Server's web interface, specifically in the loginok.html file. It allows attackers to inject arbitrary Lua code into session files, leading to remote code execution with the privileges of the FTP service (typically root or SYSTEM). Alarmingly, the flaw can be exploited via anonymous FTP accounts, making it highly accessible to threat actors.

Vulnerability Details:

- **CVE ID:** CVE-2025-47812
- **Severity:** Critical (Remote Code Execution)
- **CVSS Score:** 10.0
- **CVSS Vector:** CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H
- **Status:** Resolved
- **Workaround Available:** False
- **Exploitation Status:** Actively exploited

Affected Versions:

- Wing FTP Server < 7.4.4

Fixed Version

- Wing FTP Server ≥ 7.4.4

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the Wing FTP Servers to the latest, or patched 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-2025-47812