Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Wing FTP Flaw Enables System Takeover

Date of Publication	Admiralty Code	TA Number
July 14, 2025	A1	TA2025216

Summary

First Seen: June 2025
Affected Product: Wing FTP Server
Impact: A critical vulnerability in Wing FTP Server (CVE-2025-47812) has opened the door for attackers to take full control of affected systems. By sneaking malicious code into a login request using a null byte trick, hackers can exploit the server's session handling to execute code with high-level access. The flaw lies in how the server processes session files, inadvertently running any injected Lua script. What makes this especially dangerous is how quickly threat actors jumped on it active attacks were seen just a day after the flaw was disclosed. Adding to the urgency, a public proof-of-concept (PoC) exploit is already available, making it even easier for attackers to replicate. If you're using Wing FTP Server version 7.4.3 or earlier, updating immediately is crucial to avoid falling victim.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-47812	Wing FTP Server Remote Code Execution Vulnerability	Wing FTP Server	✗	✗	✓

Vulnerability Details

#1 Wing FTP Server, a widely used cross-platform solution supporting protocols like FTP, FTPS, HTTP, HTTPS, and SFTP, has been found vulnerable to a critical remote code execution flaw, tracked as CVE-2025-47812. This flaw stems from a weakness in the authentication process, specifically within the /loginok.html endpoint.

#2 The flaw can be exploited by injecting a null byte into the username field, which effectively tricks the server into bypassing proper authentication checks. Once this is done, the manipulated username containing the null byte and attacker-supplied Lua code is saved directly into the user session file without any sanitization. These session files, stored with .lua extensions in the server's session directory, are later executed by the Wing FTP service as part of its normal session handling process.

#3 Because these .lua files are interpreted as code, the malicious payloads embedded in them run automatically once the session is loaded. The attackers don't just gain access they gain complete control of the host system, with no need for further privilege escalation. It's an immediate pathway to full system compromise.

#4 Exploitation in the wild began rapidly, real-world attacks were observed just one day after the flaw was publicly disclosed. Threat actors were seen actively scanning for and compromising vulnerable systems. Early-stage activity included multiple IPs probing victim servers, followed by the execution of reconnaissance commands, creation of new user accounts for persistence, and the use of tools like certutil to download additional malware. Attackers also tested connections to webhook services, confirming successful infections and exfiltration capabilities.

#5 For organizations using Wing FTP Server, this is a red-alert situation. The fix is available in version 7.4.4, and updating immediately is the only effective way to shut down this threat. Leaving servers unpatched puts critical infrastructure and sensitive data at serious risk of compromise.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-47812	Wing FTP Server before 7.4.4	cpe:2.3:a:wftpserver:wing_ftp_server:*:*:*:*:*:*:*:*	CWE-158

Recommendations

Update Immediately: Install the latest version of Wing FTP Server (7.4.4 or newer) right away. This version includes a fix for the vulnerability and is your best defense against attackers exploiting it.

Limit Internet Exposure: If your Wing FTP login interface is accessible from the internet, restrict access. Only allow trusted IP addresses or put the server behind a VPN or firewall to reduce the risk of outside attacks.

Monitor for Suspicious Activity: Keep an eye on logs for strange usernames or login attempts especially those with weird characters or failed logins. This could be an early sign of someone trying to exploit the bug.

Scan for Unusual Session Files: Regularly check the server's session folder (e.g., session/ directory) for unexpected .lua files. These could contain injected code and may indicate a compromise.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
T1059 Command and Scripting Interpreter	**T1136** Create Account	**T1068** Exploitation for Privilege Escalation	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	223[.]160[.]131[.]104, 149[.]248[.]44[.]88, 103[.]88[.]141[.]42, 185[.]196[.]9[.]225, 146[.]70[.]11[.]39
URLs	hxxps[:]//webhook[.]site/5d112487-6133-4942-ac87-3f473d44bd81, hxxp[:]//185[.]196[.]9[.]225[:]8080/EOp45eWLSp5G5Uwp_yOCiQ %TEMP%\\mvveiWJHx[.]exe, hxxps[:]//ooooooo11[.]screenconnect[.]com/bin/screenconnect[.]clientsetup[.]msi, instance-y9tbyl-relay[.]screenconnect[.]com
SHA256	c637ec00bd22da4539ec6def89cd9f7196a303d17632b1131a89d65e4f5698f4, f0fcc638cd93bdd6fb4745d75b491395a7a1b2cb08e0153a2eb417cb2f58d8ac
File Path	%TEMP%\\mvveiWJHx.exe, c:\1.msi

Patch Details

Install the latest version of Wing FTP Server (7.4.4 or newer) to address the flaw.

Link: https://www.wftpserver.com/download.htm

References

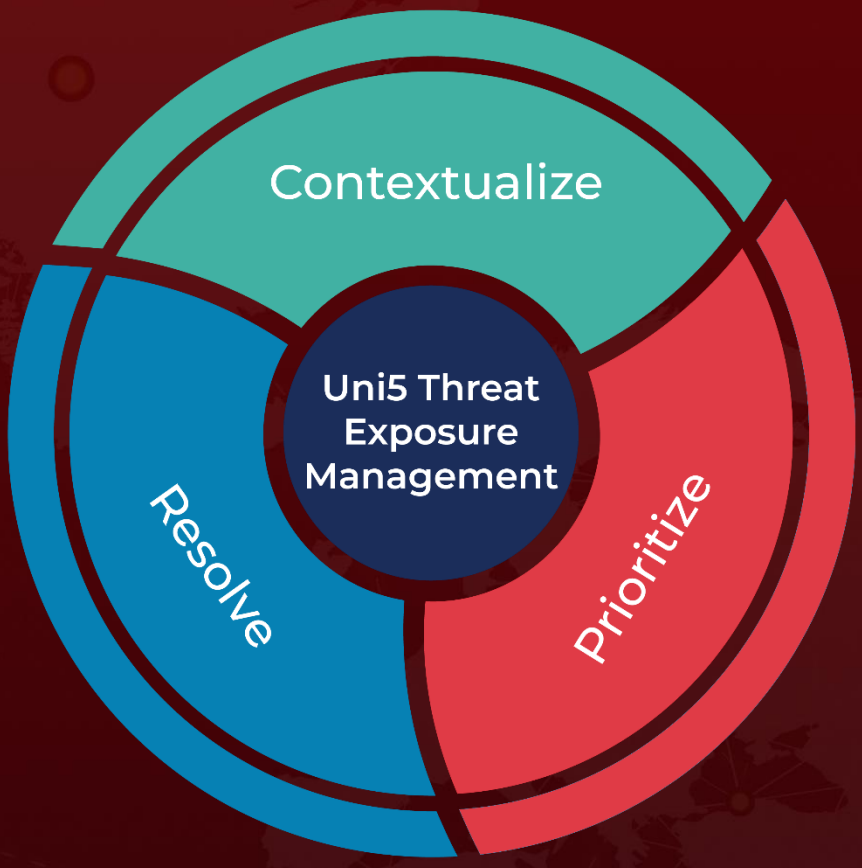
https://www.huntress.com/blog/wing-ftp-server-remote-code-execution-cve-2025-47812-exploited-in-wild

https://www.rcesecurity.com/2025/06/what-the-null-wing-ftp-server-rce-cve-2025-47812/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

July 14, 2025 • 6:00 AM

More at www.hivepro.com