



NCSC-2025-0230

Kwetsbaarheid verholpen in Wing FTP Server

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 14-07-2025

TLP:WHITE

Toegestane verspreiding van TLP:WHITE

(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

De ontwikkelaar van Wing FTP Server heeft een kwetsbaarheid verholpen in versie 7.4.4.

Duiding

De kwetsbaarheid bevindt zich in de wijze waarop Wing FTP Server null bytes verwerkt in de user parameter. Dit stelt een kwaadwillende op afstand in staat om willekeurige Lua-code te injecteren in sessie bestanden, wat kan leiden tot de uitvoering van willekeurige code met rechten van de applicatie. Het is mogelijk dat de applicatie draait met verhoogde rechten, waardoor code executie mogelijk is onder ROOT/SYSTEM-rechten.

Voor succesvol misbruik moet er geldige authenticatie plaatsvinden, of anonymous FTP moet ingeschakeld zijn. Standaard is anonymous FTP uitgeschakeld.

Onderzoekers hebben een exploit gepubliceerd waarmee de kwetsbaarheid kan worden misbruikt. Daarnaast melden diverse organisaties actief misbruik waar te nemen.

Oplossingen

De ontwikkelaar van Wing FTP server heeft updates uitgebracht om de kwetsbaarheid te verhelpen. Beveiligingsbedrijf Huntress heeft indicators-of-compromise (IoC's) vrijgegeven, waarmee mogelijke compromittatie kan worden ontdekt. Zie bijgevoegde referenties voor meer informatie.

Referenties

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

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-47812	10.0 CRITICAL

CWE's

CWE	Beschrijving
-----	--------------

[> CWE-158](#)

Improper Neutralization of Null Byte or NUL Character

Getroffen producten

wftpserver

Wing FTP
Server

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.