



# NCSC-2025-0101

## Kwetsbaarheid verholpen in CrushFTP

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 07-04-2025

Revisie: 1.0.1

### **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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto:info@ncsc.nl)

## Update Revisie 1

CVE-id vervangen voor officiële CVE-id voor deze kwetsbaarheid. Onderzoekers hebben PoC gepubliceerd.

## Feiten

CrushFTP heeft een kwetsbaarheid verholpen in versies 10.0.0 tot 10.8.3 en 11.0.0 tot 11.3.0.

## Duiding

De kwetsbaarheid stelt een kwaadwillende in staat om ongeauthenticeerde externe toegang te verkrijgen via HTTP-verzoeken, wat kan leiden tot ongeautoriseerde toegang. Systemen die gebruik maken van de DMZ Proxy instance van CrushFTP zijn niet kwetsbaar.

Onderzoekers hebben de patch reverse-engineered en hebben een PoC kunnen bouwen waarmee de kwetsbaarheid kan worden aangetoond.

Het NCSC ontvangt meldingen dat kwaadwillenden actief scannen naar kwetsbare systemen en dat compromittaties worden waargenomen.

Eigenaren van een systeem dat gebruik maakt van CrushFTP kunnen detecteren of eventuele compromittatie heeft plaatsgevonden, door in de `session_logs` directory te controleren of externe toegang is verkregen op standaard accounts als `crushadmin` of `anonymous`. Logregels als voorbeeld zijn:

```
SESSION|03/27/2025 12:41:24.636| [HTTP:250_22299:crushadmin:REDACTED_ATTACKER_IP] WROTE: *230 Password OK. Co
```

```
SESSION|03/27/2025 12:41:24.636| [HTTP:250_22299:anonymous:REDACTED_ATTACKER_IP] WROTE: *230 Password OK. Co
```

N.B.: Tijdens de initiële berichtenstroom was voor deze kwetsbaarheid nog geen CVE-id toegekend. Een niet-betrokken derde partij heeft een tijdelijk CVE-id toegekend in afwachting van de definitieve versie. Deze kwetsbaarheid is daarom ook onder CVE-2025-2825 bekend.

## Oplossingen

CrushFTP heeft updates uitgebracht om de kwetsbaarheid te verhelpen. Zie bijgevoegde referenties voor meer informatie.

## Referenties

- <https://www.crushftp.com/crush11/wiki/Wiki.jsp?page=Update>
- <https://www.crushftp.com/version10.html>

## Kwetsbaarheden

CVE	CVSS Score
<a href="#">&gt; CVE-2025-31161</a>	<b>9.2 CRITICAL</b>

## CWE's

CWE	Beschrijving
<a href="#">&gt; CWE-287</a>	Improper Authentication

## Getroffen producten

<b>CrushFTP</b>
CrushFTP
<b>Crushftp</b>
Crushftp

## 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.