



NCSC-2025-0234

Kwetsbaarheid verholpen in CrushFTP

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 28-08-2025

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).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Update Revisie 1

Er worden diverse Proof-of-Concepts (PoC) gepubliceerd.

Feiten

CrushFTP heeft een kwetsbaarheid verholpen in versies 10 tot en met 10.8.5 en 11 tot en met 11.3.4_23.

Duiding

De kwetsbaarheid bevindt zich in de AS2-validatie van CrushFTP. Deze kwetsbaarheid stelt een aanvaller in staat om via HTTPS administratieve toegang te verkrijgen, vooral wanneer de DMZ-proxyfunctie niet wordt gebruikt. De kwetsbaarheid is actief misbruikt, met meldingen die in juli 2025 zijn verschenen. Ongeautoriseerde toegang kan leiden tot verdere exploitatie van de getroffen systemen.

Diverse onderzoekers publiceren inmiddels Proof-of-Concept-code (PoC) waarmee de kwetsbaarheid kan worden aangetoond. Daadwerkelijk misbruik is op dit moment nog niet eenvoudig te realiseren, omdat een zgn. 'Race condition' moet worden gerealiseerd. Het NCSC acht het waarschijnlijk dat op korte termijn werkende exploitcode wordt gepubliceerd, waarmee grootschalig misbruik eenvoudiger wordt.

Oplossingen

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

Referenties

➤ <https://www.crushftp.com/crush11wiki/Wiki.jsp?page=CompromiseJuly2025>

Kwetsbaarheden

| CVE | CVSS Score |
|----------------------------------|------------|
| ➤ CVE-2025-54309 | |

CWE's

| CWE | Beschrijving |
|-------------------------|-------------------------------|
| CWE-420 | Unprotected Alternate Channel |

Getroffen producten

| |
|-----------------|
| CrushFTP |
| 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.