Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Update Revisie 1

CVE-id vervangen voor officiele 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.  Cor
```

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/crush11wiki/Wiki.jsp?page=Update
- https://www.crushftp.com/version10.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-31161	9.2 CRITICAL

CWE's

CWE	Beschrijving
CWE-287	Improper Authentication

Getroffen producten

CrushFTP
CrushFTP
Crushftp
Crushftp

Disclaimer