CERT-EU

Security Advisory 2025-028

CrushFTP zero-day exploited in the wild

2025-07-24 — v1.0

TLP:CLEAR

History:

- *24/07/2025 — v1.0 – Initial publication*

Summary

CrushFTP is warning that threat actors are actively exploiting a zero-day vulnerability tracked as CVE-2025-54309, which allows attackers to gain administrative access via the web interface on vulnerable servers [2, 3]. Threat actors were first detected exploiting the vulnerability on July 18th at 9AM CST, though it may have begun in the early hours of the previous day [1].

Techincal details

The attack occurs via the software's web interface in versions prior to CrushFTP v10.8.5 and CrushFTP v11.3.4_23. It is unclear when these versions were released, but CrushFTP says around July 1st [1].

Enterprise customers using a DMZ CrushFTP instance to isolate their main server are not believed to be affected by this vulnerability.

Accoring to CrushFTP:

> We believe this bug was in builds prior to July 1st time period roughly... the latest versions of CrushFTP already have the issue patched. The attack vector was HTTP(S) for how they could exploit the server. We had fixed a different issue related to AS2 in HTTP(S) not realizing that prior bug could be used like this exploit was. Hackers apparently saw our code change, and figured out a way to exploit the prior bug.

Affected products

- CrushFTP version 10 below 10.8.5
- CrushFTP version 11 below 11.3.4_23

Recommendations

Check if you may have been compromised. IoC include [1]:

- your `MainUsers/default/user.XML` contains `last_logins`
- the modified date on your default `user.XML` is recent
- default user has admin access
- long random userid's created you don't recognise - example: `7a0d26089ac528941bf8cb998d97f408m`
- other usernames recently created with admin access.
- buttons from the end-user web interface disappeared, and formerly regular user now has `Admin` button

In case of compromise [1]:

- Restore a prior default user from your backup folder from before the exploit. (`<CrushFTP folder>/backup/users/MainUsers/default/..`). You can also just delete your default user and CrushFTP will re-create it for you, but you won't have any prior customizations you might have done.
- Restore it to your `<CrushFTP folder>/users/MainUsers/default`
- Review upload/download reports for anything transferred. Hackers re-used scripts from prior exploits to deploy things on CrushFTP servers. We recommend restoring to July 16th time period just to avoid anything that might have been done.

References

[1] https://www.crushftp.com/crush11wiki/Wiki.jsp?page=CompromiseJuly2025

[2] https://www.bleepingcomputer.com/news/security/new-crushftp-zero-day-exploited-in-attacks-to-hijack-servers/

[3] https://www.rapid7.com/blog/post/crushftp-zero-day-exploited-in-the-wild/