Security Advisory 2025-015

Critical vulnerability in CrushFTP

2025-04-03 — v1.0

TLP:CLEAR

History:

- *03/04/2025 — v1.0 – Initial publication*

Summary

In April 2025, information about an easy-to-exploit critical vulnerability affecting CrushFTP was made public. It is recommended updating affected server as soon as possible [1,2].

Proof of concepts are available, and the vulnerability is being exploited in the wild.

Technical Details

Due to failures in the vulnerability disclosure process, the vulnerability has been assigned more than one CVE identifiers, i.e. **CVE-2025-31161** and **CVE-2025-2825**, with a CVSS score of 9.8.

The vulnerability is an authentication bypass vulnerability in the AWS4-HMAC authorisation method of the HTTP component of the CrushFTP server [2].

Affected Products

The vulnerability affects CrushFTP version 10 (prior to 10.8.4) and 11 (prior to 11.3.1)

Recommendations

CERT-EU recommends updating the affected products to the latest version as soon as possible.

References

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

[2] https://outpost24.com/blog/crushftp-auth-bypass-vulnerability/