Contents

CrushFTP auth bypass vulnerability: Disclosure mess leads to attacks

Application Security • Cybersecurity News • Last updated: 02 Apr 2025

Written By

Kristian Varnai
Senior Security Consultant, Outpost24

Marcus White
Cybersecurity Specialist, Outpost24

Outpost24 analysts recently discovered a critical authentication bypass vulnerability in CrushFTP, identified as CVE-2025-31161. The vulnerability has a CVSSv3.1 score of **CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (9.8)**. We reached out to MITRE for a CVE on 13th March 2025 and were within an agreed 90-day non-disclosure period with CrushFTP. The plan was to give users plenty of time to patch before attackers were alerted to the vulnerability and able to exploit it.

Unfortunately, other parties have circulated news of the vulnerability under a separate CVE (CVE-2025-2825) without cooperating with Outpost24 and CrushFTP. This means the vulnerability has not been disclosed in a secure manner as intended.

CrushFTP vulnerability is now being used in attacks

The vulnerability is now being exploited by remote attackers, who are using it to gain unauthenticated access to devices running unpatched versions of CrushFTP v10 or v11. There have been over 1,500 vulnerable instances exposed online. The threat is particularly concerning as file transfer products like CrushFTP are often targeted by ransomware gangs.

CrushFTP has released patches to address the issue, and the recommended action is to immediately update to version 10.8.4 or 11.3.1 and later. “Please take immediate action to patch ASAP. The bottom line of this vulnerability is that an exposed HTTP(S) port could lead to unauthenticated access,” CrushFTP warned in an email sent to customers on Friday, March 21st, when it released patches to address the security flaw. If immediate patching isn’t possible, enabling the DMZ perimeter network option can serve as a workaround.

We’ll run through how the vulnerability works, how our analysts found it, and the timeline of events around the botched disclosure of this issue.

CrushFTP vulnerability (CVE-2025-31161) summary

- **Where does the vulnerability exist?** The HTTP Authorization header in CrushFTP

- **What does it target?** Support for AWS4-HMAC-SHA256 authentication, intended for Amazon services

- **How is authentication bypassed?** The server obtains user information by requesting the internal authentication mechanism to authenticate the supplied user without any password. This temporarily authenticates the user (any user, including administrators) and ties it to the supplied session. If incorrect authentication data is supplied, the server is then intended to invalidate the session, but it still means that the session IS authenticated with an arbitrary user for a brief period of time

- **How hard is the bypass to execute?** This is called a race condition and is normally difficult to execute, due to requiring the hitting of a very narrow time window. The session can, however, be made permanent by sending a mangled Authorization header, which causes the request to finish with an error before it can invalidate the session

- **Is the vulnerability dangerous?** Due to the fact that most people choose the suggested “crushadmin” user as their admin user, or other easily guessable usernames, this makes the vulnerability very dangerous as it can very easily give anyone administrative access to CrushFTP

How the CrushFTP auth bypass vulnerability works

A race condition exists in the AWS4-HMAC authorization method of the HTTP component of the FTP server. The server first verifies the existence of the user by performing a call to **login_user_pass()** with no password requirement. This will authenticate the session through the HMAC verification process and up until the server checks for user verification once more.

The vulnerability can be further stabilized, eliminating the need for successfully triggering a race condition, by sending a mangled **AWS4-HMAC header**. By providing only the username and a following slash (/), the server will successfully find a username, which triggers the successful **anypass authentication process**, but the server will fail to find the expected **SignedHeaders entry**, resulting in an index-out-of-bounds error that stops the code from reaching the session cleanup.

Together, these issues make it trivial to authenticate as any known or guessable user (e.g. crushadmin) and can lead to a full compromise of the system by obtaining an administrative account.

Messy disclosure of (CVE-2025-31161): Timeline of events

- **13th March 2025:** Outpost24 requests a CVE number from MITRE

- **18th March 2025:** We contact CrushFTP about the finding

- **19th March 2025:** Outpost24 met with CrushFTP CEO Ben Spink about the technical details and CrushFTP promptly created a patch

- **20th & 24th March 2025:** We again met with CrushFTP to discuss the disclosure. Given the severity of the finding, it was important to ensure CrushFTP users were not quickly exploited if details of the vulnerability emerged. We agreed to give the full 90-day leeway in the Outpost24 disclosure guidelines so that CrushFTP users had ample time to safely upgrade

- **26th March 2025:** VulnCheck releases a CVE for the vulnerability (CVE-2025-2825). However, they had not contacted CrushFTP or Outpost24 beforehand to see if a responsible disclosure process was already underway. Nor did they credit Outpost24 for discovery. Instead, VulnCheck contacted Ben Spink to tell him they had released the CVE, after which they decided to publicly share his email in response

- **27th March 2025:** MITRE assigns us a separate CVE number: CVE-2025-31161

- **28th March 2025:** News about the vulnerability starts circulating, with others capitalizing on it by figuring out the vulnerability, writing blog posts, and releasing PoC code for it. We raised an issue ticket with MITRE regarding this issue and are currently waiting on a formal response. Unfortunately, we have seen CrushFTP's initial fears confirmed, as users are exploited in the wild.

How to recreate the CrushFTP issue

Outpost24 didn't plan to share these details at this stage but we have decided to do so since the information has already been leaked. Below are the step-by-step instructions to recreate the issue:

1. Generate a random alphanumeric session token of a minimum 31 characters of length. This is necessary to stabilize the vulnerability, as using an already existing, server-created session is volatile.

2. Set a cookie called CrushAuth to the value generated in step 1.

3. Set a cookie called currentAuth to the last 4 characters of the value generated in step 1.

4. Perform an HTTP GET request to the target /WebInterface/function/ with the cookies from steps 2 and 3, as well as an Authorization header

set to “AWS4-HMAC=<username>/”, where <username> is the user you wish to authenticate as (e.g. crushadmin).

5. The session you generated in step 1 should now be authenticated as your chosen user, you can now execute any commands that user has rights to.

Actions organizations using CrushFTP should take now

Users should immediately be patching to CrushFTP versions 10.8.4 or 11.3.1 and later. There are already cases of this vulnerability being exploited in the wild by remote attackers. If it’s not possible to immediately patch, enabling the DMZ perimeter network option can serve as a workaround.

Protect your web apps from future vulnerabilities

Outpost24’s new CyberFlex solution offers continuous visibility and monitoring of your entire application attack surface, complete with flexible, consumption-based budgeting options for a data-driven AppSec program. Get a live demo.

FAQs

What’s CrushFTP?

CrushFTP is a file transfer server software designed to provide secure and efficient file sharing over the internet. It supports a wide range of protocols, including FTP, SFTP, FTPS, HTTP, HTTPS, and WebDAV, making it suitable for various use cases, from simple file sharing to complex enterprise environments.

What’s (CVE-2025-31161)?

A vulnerability remote attackers can use to gain unauthenticated access to devices running unpatched versions of CrushFTP v10 or v11.

What should CrushFTP users do regarding (CVE-2025-31161)?

The vulnerability is now being exploited by remote attackers, so users should immediately patch to 10.8.4 or 11.3.1 and later.

About the Author

Kristian Varnai
Senior Security Consultant, Outpost24

Kristian is an experienced OffSec penetration tester and security researcher at Outpost24.

Marcus White
Cybersecurity Specialist, Outpost24

Marcus is an Outpost24 cybersecurity specialist based in the UK, with 8+ years experience in the tech and cyber sectors. He writes about attack surface management, application security, threat intelligence, and compliance.

Contact Us

Follow Us

Pricing

Outscan NX

SWAT

Cyber Threat Intelligence

Sweepatic

Sweepatic platform

Specops Software (an Outpost24 company)

ABOUT US

Our Company

Customers

Partners

Certifications

Careers

LEGAL

Legal Information

Website Terms of Use

Security and Policies

Privacy Statement

© Outpost24 All rights reserved.