

【已复现】CrushFTP条件竞争导致的任意管理员用户添加漏洞（CVE-2025-54309）被在野积极利用

为什么写这篇文章

近日刷到了CrushFTP曝出了一个任意管理员添加漏洞，但是看了网上Watchtowr安全团队公布的POC却只是一个示意POC（只能列出当前存在的用户）。

POC地址：<https://github.com/watchtowrlabs/watchTowr-vs-CrushFTP-Authentication-Bypass-CVE-2025-54309/>

 README

1

Detection in Action

```
python3 watchTower-vs-CrushFTP-CVE-2025-54309.py http://127.0.0.1:8082  
[*] Generated new c2f value: 6XQ0
```

watchTower-vs-CrushFTP-CVE-2025-54309.py

(*) CrushFTP Authentication Bypass Race Condition PoC

- Sonny , watchTowr (sonny@watchTowr.com)

CVEs: [CVE-2025-54309]

[*] CRUSHFTP RACE CONDITION POC
[*] TARGET: http://127.0.0.1:8082

```
[*] ENDPOINT: CrushFTP WebInterface getUserList  
[*] ATTACK: 5000 requests with new c2f every 50 requests
```

Starting race with 5000 request pairs...

[*] Generated new c2f value: qUwd

[*] NEW SESSION: c2f=qUwd

[*] EXECLITED 3 USERS: crushadmin, default, TempAccount

[*] VIII NERABIE! RACE CONDITION POSSIBLE!

在本地搭建环境进行研究，成功研究出可以添

于是在本地搭建环境进行研究，成功研究出可以添加任何管理员用户的POC。

The screenshot shows a web-based administration interface for CrushFTP. On the left, there's a sidebar with buttons for 'Files', 'Server Admin', 'Jobs', and 'User Manager'. The 'User Manager' tab is active. A sub-menu for 'User connection group' shows 'MainUsers'. Below this are buttons for 'Add', 'Copy', and 'Delete'. There are also fields for 'Filter' and 'Inheritance', and a dropdown for 'Group' set to 'All Users'. At the bottom of the sidebar are 'Reload', 'Select all', and 'none' buttons. The main area displays a list of users with columns for 'Name', 'Status', and 'Actions'. One user, 'a1batr0ss', is highlighted with a red border. The terminal output on the right shows the command being run: 'python CVE-2025-54309.py http://127.0.0.1:8080'. It includes log messages about condition competition, the target URL, and a success message: '[SUCCESS] 管理员用户已经成功添加！'. A red box highlights the success message and the newly created user information: '用户名: a1batr0ss' and '密码: TianWeng-Security'.

漏洞介绍

CrushFTP 是一款跨平台的企业级文件传输服务器软件，支持 FTP、FTPS、SFTP、HTTP(S)、WebDAV 等多种协议，能够运行在 Windows、Linux、macOS 等环境中。它提供用户友好的 Web 管理界面，支持高并发文件传输、压缩与解压缩、自动化任务、事件触发、日志审计和权限管理等功能。相比传统 FTP 服务器，CrushFTP 更强调安全性和可扩展性，常用于企业内部文件共享、对外数据交换以及自动化传输流程的搭建。



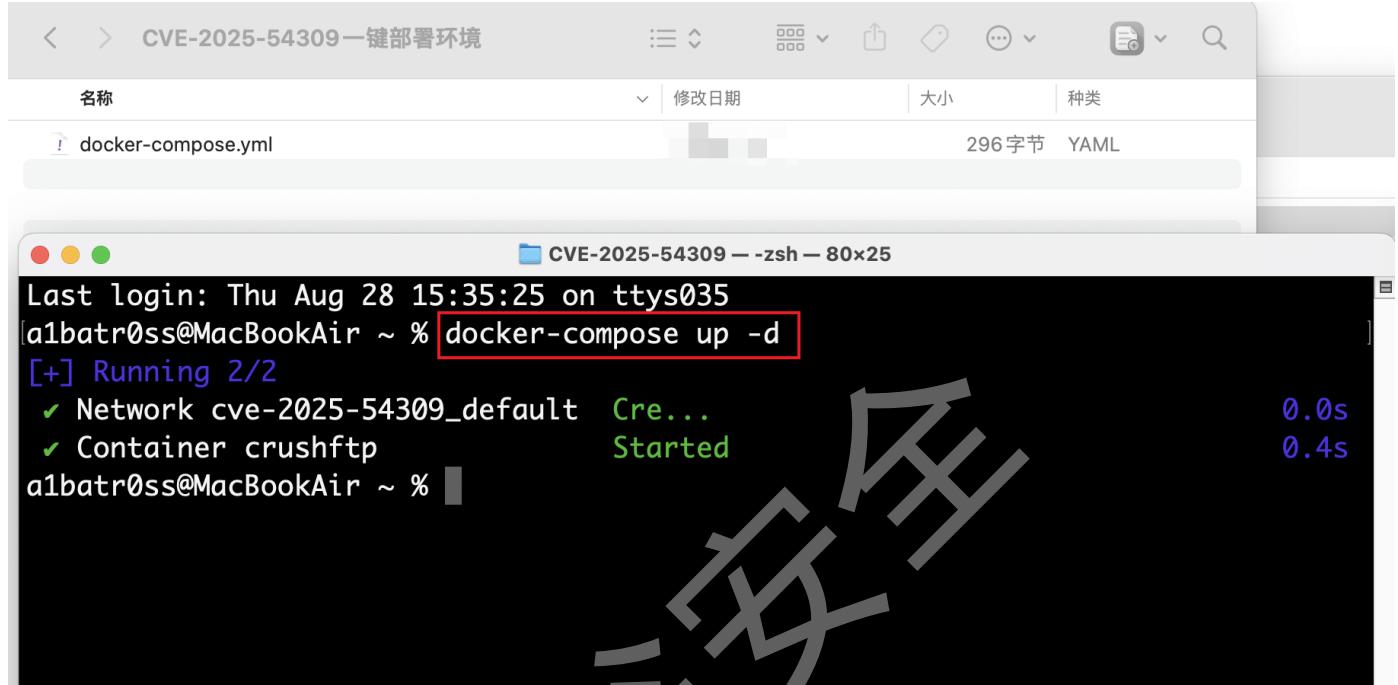
CVE-2025-54309 是 CrushFTP 中的一个严重漏洞（CVSS 评分高达 9.0+），影响 10.8.5 之前的 10.x 版本和 11.3.4_23 之前的 11.x 版本。CrushFTP 在处理 AS2 验证逻辑上存在缺陷，攻击者可通过精心构造的请求绕过认证，获取管理员权限。该漏洞已在 2025 年 7 月被黑客在实际攻击中利用，危害范围广泛，官方已发布修复版本，受影响用户需立即升级并加强防护。

漏洞版本

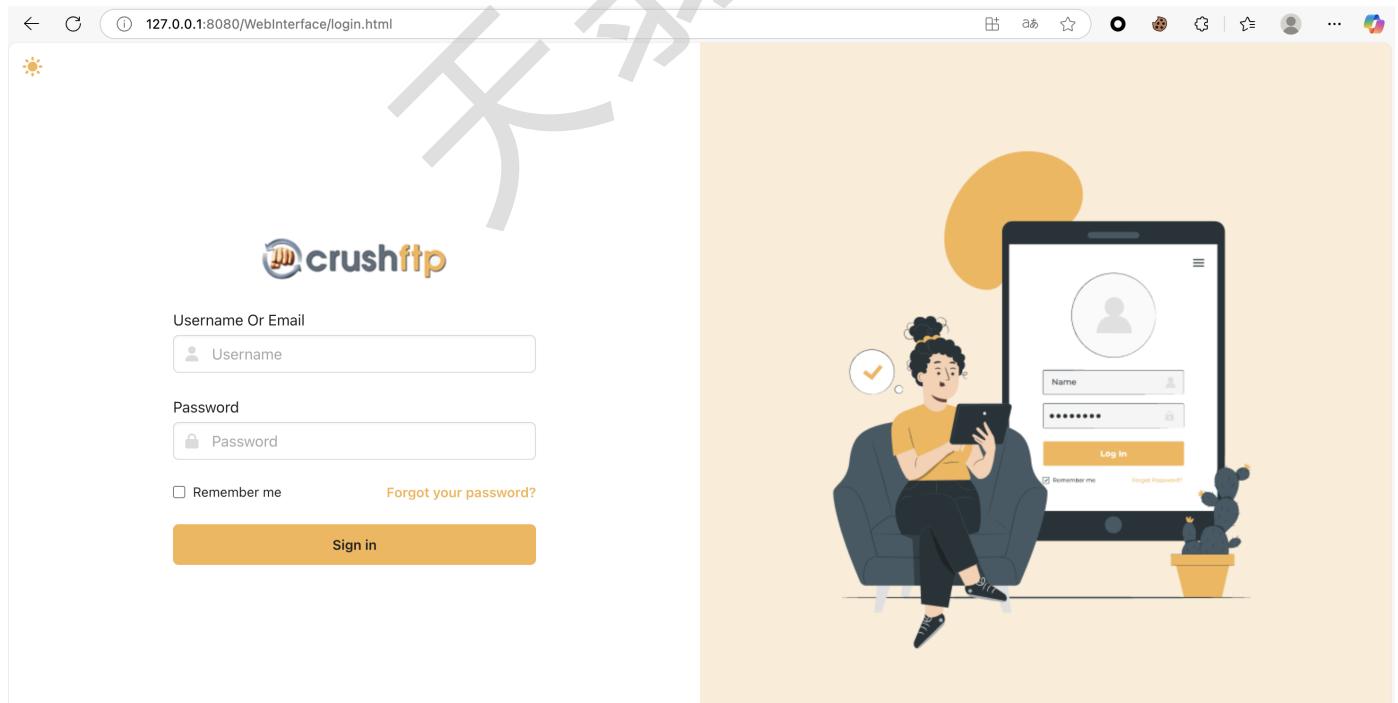
- 10.x 版本: < 10.8.5版本
- 11.x 版本: < 11.3.4_23版本

一键部署-漏洞环境

在“CVE-2025-54309一键部署环境”文件夹执行 `docker-compose up -d` 即可部署CVE-2025-54309漏洞环境



CVE-2025-54309环境搭建完成后，访问 <http://127.0.0.1:8080> 即可看到CrushFTP后台的web界面，



漏洞利用

执行一下命令对目标环境进行CVE-2025-54309漏洞利用，执行成功后会给CrushFTP增加一个用户名为a1batr0ss、密码为TianWeng-Security的管理员用户。

```
python CVE-2025-54309.py 【CrushFTP的地址】
```

```
(CommonPython) a1batr0ss@MacBookAir ~ % python CVE-2025-54309.py http://127.0.0.1:8080
[*] CrushFTP条件竞争导致的任意管理员用户添加漏洞 POC
[*] 目标: http://127.0.0.1:8080
开始进行条件竞争漏洞利用尝试, 这会需要一些时间...
[SUCCESS] 管理员用户已经成功添加!
```

用户名: a1batr0ss
密码: TianWeng-Security

我们利用刚才生成的管理员a1batr0ss的用户名和密码，可以成功登录到CrushFTP的后台

The screenshot shows the CrushFTP web interface at <http://127.0.0.1:8080/WebInterface/UserManager/index.html>. The 'User Manager' tab is active. A user entry for 'a1batr0ss' is highlighted with a red box. The interface includes standard file management buttons like 'Add', 'Copy', and 'Delete'. A yellow message bar at the top right says: 'Choose user from left menu to change settings. More options available in top menu.' On the left, there's a sidebar with 'File', 'Server Admin', 'Jobs', 'User Manager' (which is orange), 'Preferences', 'Shares', 'PGP', and other icons. The 'User Manager' section has fields for 'Filter:', 'Inheritance:', and 'Group: All Users'. Below the main area, there are reload and selection buttons ('Select all', 'paste', 'none').

我们拥有的权限甚至可以把原来存在的管理员删除掉

The screenshot shows a web-based file manager interface with a navigation bar at the top containing links for Files, Server Admin, Jobs, User Manager (which is highlighted), Preferences, Shares, PGP, and other system-related options. The main content area is titled "User Settings". It displays a list of users with one user, "crushadmin", selected. A context menu is open for this user, with the "Delete Selected Users" option highlighted by a red arrow. The right side of the screen shows a "Server's Files" panel with a tree view of directory contents like app, bin, dev, etc., and a "User's Stuff" panel.

漏洞修复

修复需要将版本升级

- 10.x 版本：升级到10.8.5版本及以上
- 11.x 版本：升级到11.3.4_23版本及以上

The screenshot shows the official website for CrushFTP. At the top, there is a navigation bar with links for HOME, DOWNLOAD, OVERVIEW, FEATURES, CASE STUDIES, DOCS, PRICING, and SUPPORT. Below the navigation, there is a search bar labeled "快速导航" and a login link "您好 (匿名访客) 登录". The main content area features a prominent red box containing two warning messages: "CrushFTP 11.0.0 to 11.3.4 are vulnerable. Update to 11.3.4_23+ immediately." and "CrushFTP 10.0.0 to 10.8.4 are vulnerable. Update to 10.8.5+ immediately.". Below these messages, there is some general guidance on detection and what to do if compromised. Further down, sections include "Automated Updating" (with instructions to enable "Major Release Versions" in Preferences), "Update Bug on Windows" (describing a problem with automatic updates on Windows), and "Vulnerability Info" (mentioning a specific vulnerability related to unauthenticated HTTP(S) access using known usernames, CVE-2025-54309). The left sidebar contains links for "CrushFTP11 | What's New" (including Upgrading to CrushFTP11, FTP Proxy, Videos, Downloads, Pricing, Enterprise License Enhancements), "WebInterface" (Uploads, Downloads, Online docs, sheets and slides viewing, Login Page, Features like Custom Theme, Searching, Slide Show, Thumbnails, Filtering, Quick Preview, Sharing), "Server Admin" (Dashboard, Server Info, Log, Graphs, User Info), and "CrushFTP10 | What's New" (Upgrading to CrushFTP10, FTP Proxy, Videos, Downloads, Pricing, Enterprise License Enhancements).