

HiveForce Labs

# THREAT ADVISORY



## VULNERABILITY REPORT

### **Critical Zero-Day in CrushFTP Exposes Admin Interface**

Date of Publication

July 21, 2025

Admiralty Code

A1

TA Number

TA2025226






# Summary

**First Seen:** July 18, 2025  
**Affected Product:** CrushFTP

**Impact:** A newly discovered zero-day vulnerability, identified as CVE-2025-54309, has been found in CrushFTP, a widely used enterprise file transfer platform. This flaw lets attackers quietly gain full administrative control through the web interface, particularly in setups not using the DMZ proxy feature. The issue stems from improper handling of AS2 validation over HTTPS, and intriguingly, attackers reverse-engineered a previous patch, uncovering this overlooked weakness. With internet-facing servers especially vulnerable, this incident serves as a reminder that even well-intentioned fixes can open new doors for exploitation. CrushFTP has released critical patches, and organizations are urged to update without delay and consider enabling the DMZ proxy to reduce future exposure.

## CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-54309	CrushFTP Unprotected Alternate Channel Vulnerability	CrushFTP			

# Vulnerability Details

## #1

A newly discovered zero-day vulnerability, CVE-2025-54309, has been identified in CrushFTP, a secure enterprise file transfer solution widely used across platforms and protocols. This flaw, if left unpatched, could allow attackers to gain unauthorized administrative access through the server’s web interface. The issue affects CrushFTP version 10 (before 10.8.5) and version 11 (before 11.3.4\_23) specifically when the DMZ proxy feature is disabled, putting exposed systems at serious risk.



# #2

At the heart of the vulnerability is a flaw in AS2 (Applicability Statement 2) validation logic. When improperly handled, this allows attackers to exploit HTTPS-based endpoints. The attack doesn't rely on obscure methods instead, it uses standard web protocols (HTTP/HTTPS), making any public-facing CrushFTP servers particularly vulnerable. The discovery highlights the risks of reverse engineering, as threat actors were able to dissect changes made in earlier updates and spot this unintentional security gap.

# #3

Interestingly, a previous bug fix related to AS2 in HTTP(S) had unknowingly mitigated this zero-day. However, attackers reviewing that change were able to understand the impact and weaponize the earlier bug, exploiting it in a way that had not been previously anticipated. This highlights how even well-intentioned patches can sometimes reveal new paths for exploitation if not carefully reviewed from a security perspective.

# #4

Given that attackers are actively exploiting flaws in CrushFTP including the recently discovered CVE-2025-54309 and the earlier [CVE-2025-31161](#) patched in April, it's critical for organizations using CrushFTP to stay up to date with the latest security patches. Prioritize applying the vendor-provided patches immediately and review your deployment configurations, especially around DMZ proxy usage, to strengthen your overall security posture.

## Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-54309	CrushFTP 10 before 10.8.5 and 11 before 11.3.4_23	cpe:2.3:a:crushftp:crushftp:*:*:*:*:*	CWE-420

## Recommendations



**Update Immediately:** If you're running CrushFTP version 10 before 10.8.5 or version 11 before 11.3.4\_23, stop what you're doing and apply the latest patch right away. This fix blocks attackers from sneaking in through the web interface.



**IP Whitelisting:** Limit the IP addresses from which administrative actions can be performed on the CrushFTP server. Implement IP whitelisting to restrict which IP addresses are permitted to connect to the CrushFTP server at all.





**Use a DMZ Instance for Extra Safety:** To reduce the risk of direct attacks on your internal CrushFTP server, it's strongly recommended to deploy a DMZ (Demilitarized Zone) instance. This means placing a separate CrushFTP server at the network's edge to handle external traffic, acting as a buffer between the internet and your main/internal system.



**Automated Updates:** Ensure automatic and frequent updates are enabled within CrushFTP's preferences. This helps ensure the timely application of patches, reducing the window of vulnerability.



**Vulnerability Management:** This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.



## Potential MITRE ATT&CK TTPs

<b><u>TA0042</u></b> Resource Development	<b><u>TA0001</u></b> Initial Access	<b><u>TA0004</u></b> Privilege Escalation	<b><u>TA0005</u></b> Defense Evasion
<b><u>T1588</u></b> Obtain Capabilities	<b><u>T1588.006</u></b> Vulnerabilities	<b><u>T1190</u></b> Exploit Public-Facing Application	<b><u>T1068</u></b> Exploitation for Privilege Escalation
<b><u>T1211</u></b> Exploitation for Defense Evasion			



## Indicators of Compromise (IOCs)

TYPE	VALUE
<b>File Path</b>	MainUsers/default/user.XML
<b>User Id</b>	7a0d26089ac528941bf8cb998d97f408m





## Patch Details

Install the latest version of CrushFTP to address the flaw.

Link: <https://www.crushftp.com/download.html>

## References

<https://www.crushftp.com/crush11wiki/Wiki.jsp?page=CompromiseJuly2025>

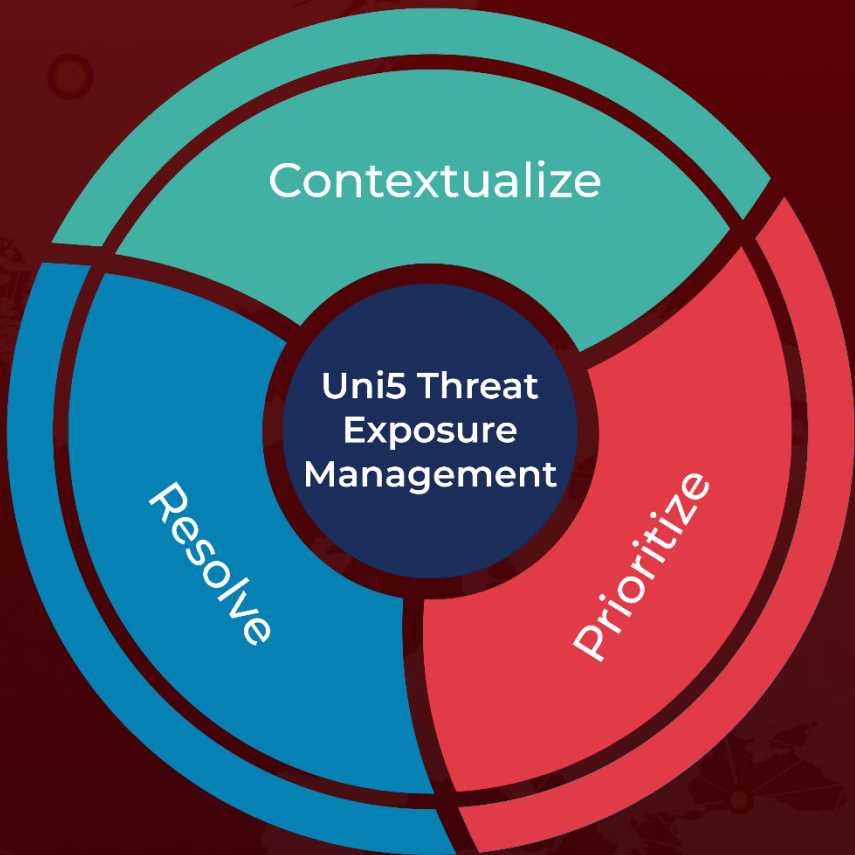
<https://hivepro.com/threat-advisory/patch-now-crushftp-authentication-bypass-actively-exploited/>



# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON  
**July 21, 2025 • 4:40 AM**

