Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Patch Now: CrushFTP Authentication Bypass Actively Exploited

Date of Publication	Last Updated date	Admiralty Code	TA Number
April 2, 2025	April 6, 2025	A1	TA2025099

Summary

First Seen: March 21, 2025
Affected Product: CrushFTP
Impact: CrushFTP, a popular file transfer server software, has a critical authentication bypass vulnerability (CVE-2025-31161) affecting versions 10.0.0-10.8.3 and 11.0.0-11.3.0. The flaw allows unauthenticated attackers to gain unauthorized server access through exposed HTTP(S) ports, potentially leading to data theft and system compromise. Active exploitation has been observed, with over 1,500 unpatched instances vulnerable. Users are strongly advised to update to versions 10.8.4 or 11.3.1 immediately to mitigate the risk.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-31161	CrushFTP Authentication Bypass Vulnerability	CrushFTP	☒	✓	✓

Vulnerability Details

#1 CrushFTP, a widely used file transfer server supporting secure protocols, has recently been found to contain a critical authentication bypass vulnerability that poses significant security risks. This vulnerability affects versions 10.0.0 through 10.8.3 and 11.0.0 through 11.3.0 of the CrushFTP file transfer software. It allows unauthenticated attackers to bypass authentication and gain unauthorized access to the server through exposed HTTP(S) ports.

#2 The flaw arises from improper handling of AWS S3-style authorization headers, enabling unauthenticated attackers to bypass authentication mechanisms. By exploiting this vulnerability, attackers can impersonate legitimate users, including administrators, and perform actions on their behalf, such as data retrieval and administrative operations.

#3

Active exploitation of this vulnerability has been observed in the wild. Attackers are leveraging publicly available proof-of-concept (PoC) exploit code to target vulnerable CrushFTP instances. Exploitation attempts have been observed primarily originating from Asia, with some from Europe and North America. Over 1,500 unpatched instances remain vulnerable as of late March 2025.

#4

The vulnerability was initially identified as CVE-2025-2825, but the National Vulnerability Database (NVD) rejected it as a duplicate. The correct and official identifier is CVE-2025-31161. CrushFTP has addressed this issue in versions 10.8.4 and 11.3.1. Users are strongly advised to update to these versions immediately to protect their systems.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-31161	CrushFTP versions 10.0.0 through 10.8.3 and 11.0.0 through 11.3.0	cpe:2.3:a:crushftp:crushftp:*:*:*:*:*:*:*	CWE-287

Recommendations

Upgrade to Patched Versions: Update CrushFTP to versions 10.8.4 or 11.3.1, which contain fixes for this vulnerability.
For instructions:

- Log in to the CrushFTP WebInterface using an admin account.
- Navigate to the About tab and select Update > Update Now

Enable DMZ Proxy (Temporary Workaround): If updating immediately is not possible, enable the DMZ (Demilitarized Zone) feature in CrushFTP. This adds an additional security layer by isolating the server from direct internet access.
Note: While helpful, this workaround does not fully mitigate the risk of exploitation.

Restrict Network Access: Limit exposure of CrushFTP servers to the internet by, restricting access to trusted IP addresses only and use a firewall or VPN to protect access to CrushFTP instances.

Secure Server Configurations: Disable insecure S3 password lookup by setting s3_auth_lookup_password_supported=false in the configuration file. Ensure proper authentication flow checks are enforced.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0004 Privilege Escalation
TA0005 Defense Evasion	T1588 Obtain Capabilities	T1588.005 Exploits	T1068 Exploitation for Privilege Escalation
T1556 Modify Authentication Process	T1190 Exploit Public-Facing Application	T1656 Impersonation	T1588.006 Vulnerabilities

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	192[.]42[.]116[.]217, 185[.]220[.]101[.]52, 192[.]42[.]116[.]212

Patch Details

Update CrushFTP instances to 10.8.4 and 11.3.1 or later.

Links:
https://www.crushftp.com/crush11wiki/Wiki.jsp?page=Update

https://www.crushftp.com/download.html

References

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

https://attackerkb.com/topics/k0EgiL9Psz/cve-2025-2825/rapid7-analysis

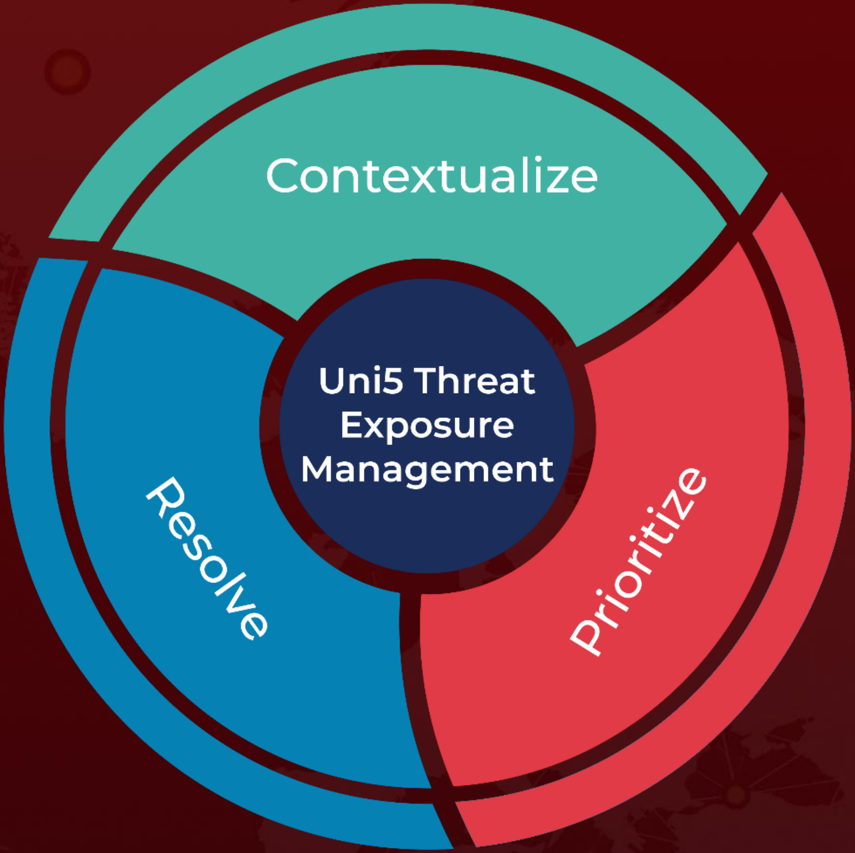
https://projectdiscovery.io/blog/crushftp-authentication-bypass

https://x.com/Shadowserver/status/1906753539499520064

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

April 2, 2025 • 9:30 PM

More at www.hivepro.com