

CVE-2025-31161

CrushFTP Authentication Bypass Vulnerability

Exigent

CISA KEV since Apr 7, 2025

Actively exploited

Ransomware use known

CrushFTP 10 before 10.8.4 and 11 before 11.3.1 allows authentication bypass and takeover of the crushadmin account (unless a DMZ proxy instance is used), as exploited in the wild in March and April 2025, aka "Unauthenticated HTTP(S) port access." A race condition exists in the AWS4-HMAC (compatible with S3) 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.

EVRS 95/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.999 99.98th percentile · FIRST	CISA DEADLINE Apr 28, 2025 KEV since 2025 · listed over a year
--	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☒ Ransomware	Known ransomware campaigns	☐ KEV recency	Added to CISA KEV within the last two years
☒ EPSS	0.999 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

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.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
crushftp	≥ 10.0.0 < 10.8.4 ≥ 11.0.0 < 11.3.1	10.8.4 · 11.3.1	NVD

Sources

Vendor guidance github.com/advisories/GHSA-c57h-rx24-vf52

Additional guidance crushftp.com/crush11wiki/Wiki.jsp?page=Update#section-Update-VulnerabilityInfo

crushftp.com crushftp.com/crush11wiki/Wiki.jsp?page=Update

NVD nvd.nist.gov/vuln/detail/CVE-2025-31161

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2025-9910

Current data evulnable.com/vulnerability-management/cve/CVE-2025-31161

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.