FORTINET

FortiGuard Labs Outbreak Alerts

CrushFTP Authentication Bypass Attack

Actively targeted File transfer solution

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

CVEs: CVE-2025-31161

FortiGuard Labs has identified ongoing and persistent attack attempts in the wild that are aimed at exploiting CVE-2025-31161, which is an authentication bypass vulnerability found in CrushFTP file transfer server. If successfully exploited, this vulnerability could allow attackers to gain administrative access to the application, representing a significant risk to enterprise environments.

Background

An attacker may take advantage of this vulnerability by sending a specifically crafted HTTP request to the CrushFTP server. If exploited, this vulnerability could result in complete system compromise. Attackers would be able to impersonate users, execute administrative actions, access sensitive information, and upload harmful content.

This vulnerability is remotely exploitable, and a proof-of-concept (PoC) exploit is now publicly accessible. This situation heightens the risk of swift adoption by threat actors, including ransomware groups that have previously targeted other Managed File Transfer (MFT) platforms such as MOVEit Transfer and Cleo MFT.

The versions affected range from 10.0.0 to 10.8.3 and from 11.0.0 to 11.3.0. Users are strongly advised to promptly update to versions 10.8.4 or 11.3.1 and later.

Latest Developments

FortiGuard Labs recommends users to apply the fix provided by the vendor and follow any instructions as mentioned on the vendor's advisory if not already done.

- April 08, 2025: FortiGuard Labs released a Threat Signal.
  https://www.fortiguard.com/threat-signal-report/6072/crushftp-authentication-bypass
- April 07, 2025: CISA Adds CVE-2025-31161 to its Known Exploited Vulnerability to Catalog.
  https://www.cisa.gov/news-events/alerts/2025/04/07/cisa-adds-one-known-exploited-vulnerability-catalog
- March 21, 2025: CrushFTP released an advisory.
  https://www.crushftp.com/crush11wiki/Wiki.jsp?page=Update

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

Lure

- FortiDeceptor

Decoy VM

- FortiDeceptor

AV

Detects known malware related to the Outbreak

- FortiADC — DB 93.02483
- FortiCASB — DB 93.02483
- FortiCWP — DB 93.02483
- FortiClient — DB 93.02483
- FortiGate — DB 93.02483
- FortiMail — DB 93.02483
- FortiProxy — DB 93.02483
- FortiSASE — DB 93.02483
- FortiWeb — DB 93.02483

Vulnerability

Detects end-user devices running the vulnerable application.

- FortiClient

AV (Pre-filter)

Detects known malware related to the Outbreak

- FortiEDR — DB 93.02483
- FortiNDR — DB 93.02483
- FortiSandbox — DB 93.02483

IPS

Detects and blocks attack attempts leveraging the vulnerability

- FortiADC — DB 31.987
- FortiGate — DB 31.987
- FortiNDR — DB 31.987
- FortiProxy — DB 31.987
- FortiSASE — DB 31.987

Web App Security

Detects and blocks attack attempts leveraging the vulnerability

- FortiWeb — DB 0.00400

DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

IOC

- FortiAnalyzer
- FortiSOCaaS
- FortiSIEM
- FortiSOAR

Outbreak Detection

- FortiAnalyzer — DB 2.00072
- FortiClient — DB 1.00030
- FortiNDR Cloud
- FortiSIEM — DB 805
- FortiSOAR

Content Update

- FortiSIEM

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automaticlly respond to this outbreak.

- FortiXDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.

- Incident Response

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.

- NSE Training
- Response Readiness

End-User Training

Raise security awareness to your employees that are continuously being targeted by phishing, drive-by download and other forms of cyberattacks.

- Security Awareness & Training

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.

- Security Rating

Vulnerability Management

Reduce the attack surface on software vulnerabilities via systematic and automated patching.

- FortiClient

Additional Resources

Vendor Update	https://www.crushftp.com/crush11wiki/Wiki.jsp?page=Update
Outpost24 Analysis	https://outpost24.com/blog/crushftp-auth-bypass-vulnerability/

Learn more about FortiGuard Outbreak Alerts