F**E**RTINET.

FortiGuard Labs Outbreak Alerts 🗘

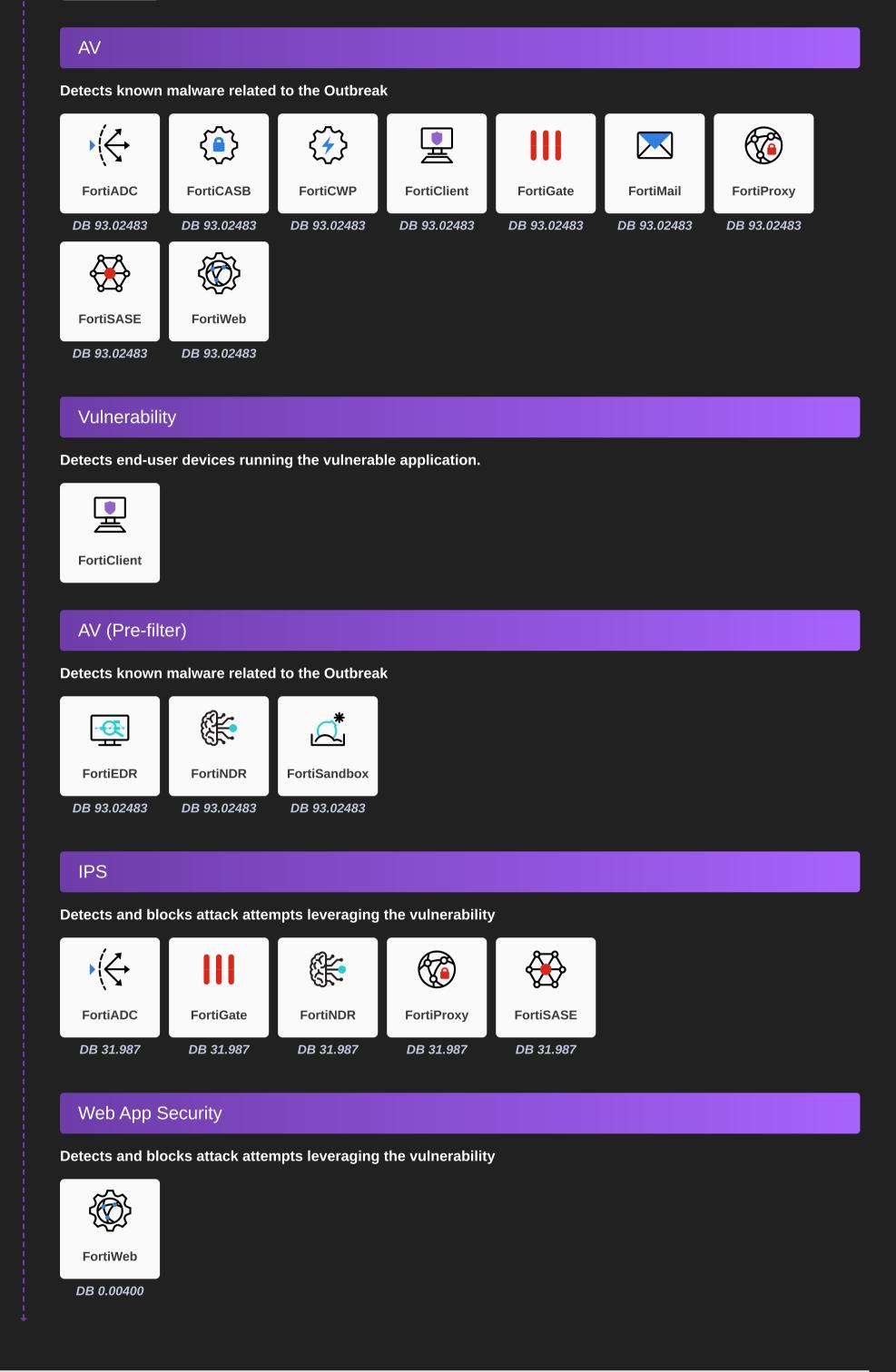
CrushFTP Authentication Bypass Attack

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. <u>https://www.fortiguard.com/threat-signal-report/6072/crushftp-authentication-bypass</u>					
	April 07, 2025: CISA Adds CVE-2025-31161 to its Known Exploited Vulnerability to Catalog. <u>https://www.cisa.gov/news-events/alerts/2025/04/07/cisa-adds-one-known-exploited-vulnerability-catalog</u>					
	March 21, 2025: CrushFTP released an advisory. https://www.crushftp.com/crush11wiki/Wiki.jsp?page=Update					
	OTECT					
Counter events:	measures across the security fabric for protecting assets, data and network from cybersecurity					
Lure						
FortiDeceptor						
Decoy VM						
FortiDeceptor						

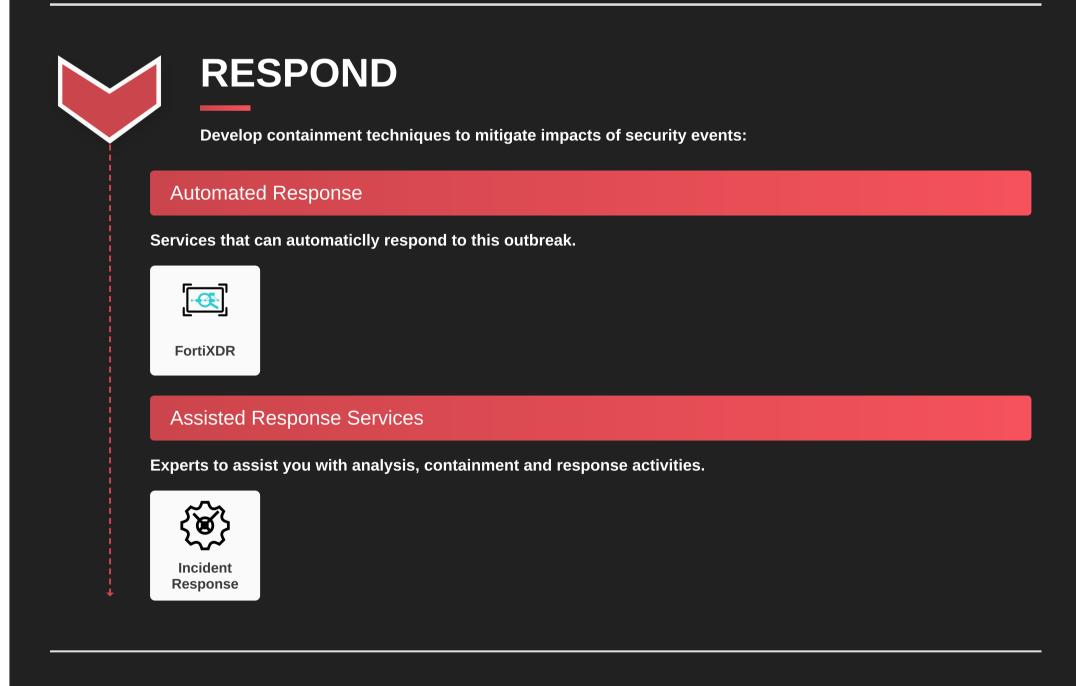






Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

IOC							
\bigcirc		ズ	(•)				
FortiAnalyzer	FortiSOCaaS	FortiSIEM	FortiSOAR				
Outbreak Detection							
	₽		ズ	٢			
FortiAnalyzer	FortiClient	FortiNDR Cloud	FortiSIEM	FortiSOAR			
DB 2.00072	DB 1.00030		DB 805		,		
Content Update							
X							
FortiSIEM							

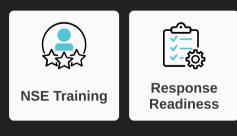


RECOVER

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

NOC/SOC Training

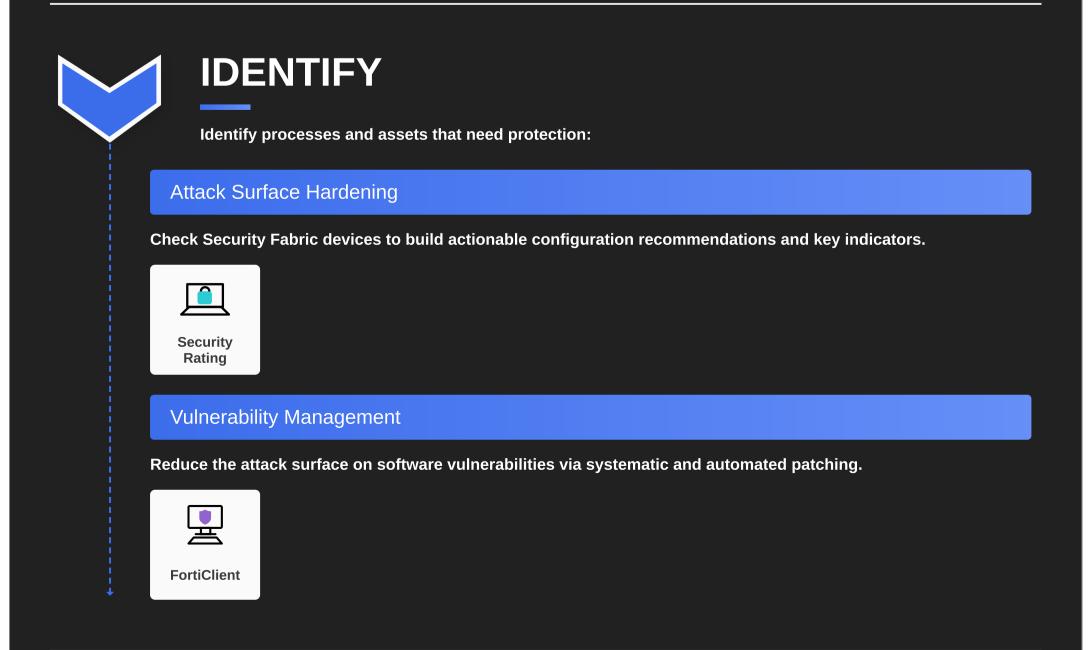
Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.



End-User Training

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





Additional Resources

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

Outpost24 Analysis <u>https://outpost24.com/blog/crushftp-auth-bypass-vulnerability/</u>

Learn more about FortiGuard Outbreak Alerts

