ColdFusion Exploit in the Wild

Posted At : November 9, 2018 1:39 PM | Posted By : Wil Genovese
Related Categories: ColdFusion, Coldfusion Security, Security

On September 11th of 2018 Adobe released a **critical security patch** to patch a very dangerous flaw (**CVE-2018-15961**) that could allow an attacker to upload a file that can be used to exploit and take control of the server. Adobe updated their security note to alert everyone that there are active exploits in the wild.

> "UPDATE: As of September 28, Adobe is aware of a report that CVE-2018-15961 is being actively exploited in the wild. The updates for ColdFusion 2018 and ColdFusion 2016 announced in this bulletin have been elevated to Priority 1. Adobe recommends customers update to the latest version as soon as possible." - Adobe

Today it is being reported by multiple news outlets including **ZDNet** that the exploit is in the wild and being used by a nation-state cyber-espionage group.

> "A nation-state cyber-espionage group is actively hacking into Adobe ColdFusion servers and planting backdoors for future operations, Volexity researchers have told ZDNet. The attacks have been taking place since late September and have targeted ColdFusion servers that were not updated with security patches that Adobe released two weeks before, on September 11." - ZDNet

This is one more friendly reminder to make sure your ColdFusion servers are patched! Either patch them yourself, have your hosting provider patch them or if they are not familiar or knowledgeable with ColdFusion contact us at **CF Webtools** to patch your servers. Our operations group is standing by 24/7 - give us a call at 402-408-3733, or send a note to "operations at cfwebtools.com".