

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## **Active Exploitation of Adobe ColdFusion Critical Vulnerabilities**

Date of Publication

July 18, 2023

Admiralty Code

A1

TA Number

TA2023302










# Summary

**First Seen:** July 11, 2023

**Affected Platforms:** Adobe ColdFusion

**Impact:** These vulnerabilities allow attackers to bypass authentication, execute remote code, and gain unauthorized access to vulnerable servers.

## CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-29298	Adobe ColdFusion Improper Access Control Vulnerability	Adobe ColdFusion			
CVE-2023-38203	Adobe ColdFusion Arbitrary Code Execution Vulnerability	Adobe ColdFusion			
CVE-2023-29300	Adobe ColdFusion Deserialization of Untrusted Data Vulnerability	Adobe ColdFusion			

## Vulnerability Details

# #1

Threat actors are actively exploiting two critical vulnerabilities in ColdFusion, a web application development platform. The first vulnerability (CVE-2023-29298) allows them to bypass authentication and gain unauthorized access, while the second one (CVE-2023-38203) enables remote code execution, giving them control over vulnerable servers.

## #2

Adobe released a patch to address CVE-2023-29298, but it was later found to be bypassable. Additionally, a proof-of-concept exploit for CVE-2023-29300, a deserialization vulnerability allowing remote code execution. Attackers are combining these exploits to install webshells on vulnerable ColdFusion servers, granting them remote access. These webshells have been found in the folder path: `.\ColdFusion11\cfusion\wwwroot\CFIDE\ckeditr.cfm`.

## #3

The attacker's behavior involves sending POST requests to `accessmanager.cfc` in IIS logs to exploit the vulnerability. They then execute encoded PowerShell commands to create a webshell, often observed in the `\wwwroot\CFIDE` directory. Additionally, cURL commands to a specific Burpsuite URL and activity related to querying the domain controller with `nltest /domain_trusts` have been observed.

## Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-29298	Adobe ColdFusion 2018: Update 17 and earlier versions	<code>cpe:2.3:a:adobe:coldfusion:2023.*.*.*.*.*</code>	CWE-254
CVE-2023-38203	Adobe ColdFusion 2021: Update 7 and earlier versions	<code>cpe:2.3:a:adobe:coldfusion:2023:Update 1.*.*.*.*.*</code>	CWE-502
CVE-2023-29300	Adobe ColdFusion 2023: Update 1 and earlier versions	<code>cpe:2.3:a:adobe:coldfusion:2023.*.*.*.*.*</code>	CWE-502

# Recommendations



**Apply Patches and Updates:** Immediately apply the latest security patches provided by Adobe for both CVE-2023-29298 and CVE-2023-38203. Ensure that all ColdFusion installations are up-to-date with the latest fixes to eliminate known vulnerabilities.



**Implement Lockdown Mode:** Enable ColdFusion's lockdown mode to restrict access to critical functionality and reduce attack surfaces. Lockdown mode helps prevent direct access to pre-auth CFC endpoints, which can be targeted in combination with the vulnerabilities. This measure can significantly enhance the security of your ColdFusion deployment.



**Monitor and Review Logs Regularly:** Continuously monitor your ColdFusion server logs, especially IIS logs, for suspicious POST requests or any other unusual activity related to the vulnerabilities. This proactive monitoring can help detect and respond to potential attacks in a timely manner.



## Potential MITRE ATT&CK TTPs

<b><u>TA0001</u></b> Initial Access	<b><u>TA0002</u></b> Execution	<b><u>TA0003</u></b> Persistence	<b><u>TA0042</u></b> Resource Development
<b><u>T1190</u></b> Exploit Public-Facing Application	<b><u>T1059.001</u></b> PowerShell	<b><u>T1059</u></b> Command and Scripting Interpreter	<b><u>T1505.003</u></b> Web Shell
<b><u>T1505</u></b> Server Software Component	<b><u>T1588</u></b> Obtain Capabilities	<b><u>T1588.005</u></b> Exploits	<b><u>T1588.006</u></b> Vulnerabilities
<b><u>T1203</u></b> Exploitation for Client Execution			

## Indicators of Compromise (IOCs)

TYPE	VALUE
<b>IPV4</b>	62.233.50[.]13 5.182.36[.]4 195.58.48[.]155
<b>Domains</b>	oastify[.]com ckeditr[.]cfm
<b>SHA256</b>	08D2D815FF070B13A9F3B670B2132989C349623DB2DE154CE43989BB4 BBB2FB1

## Patch Details

<https://helpx.adobe.com/security/products/coldfusion/apsb23-40.html>

<https://helpx.adobe.com/security/products/coldfusion/apsb23-41.html>

## References

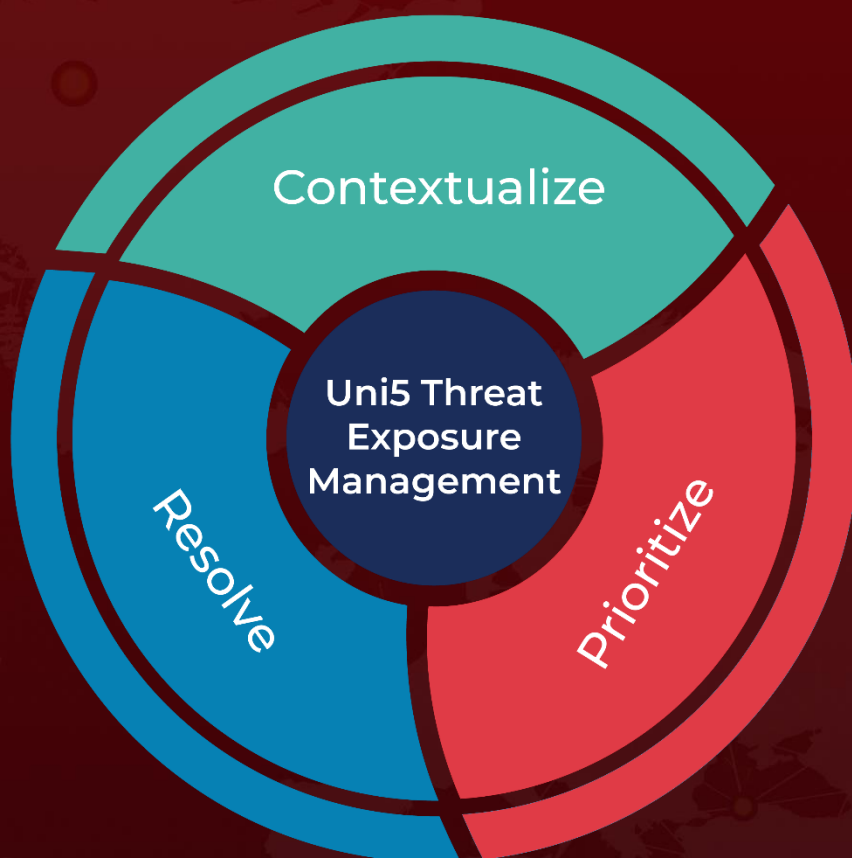
<https://www.rapid7.com/blog/post/2023/07/17/etr-active-exploitation-of-multiple-adobe-coldfusion-vulnerabilities/>

<https://www.rapid7.com/blog/post/2023/07/11/cve-2023-29298-adobe-coldfusion-access-control-bypass/>

# 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

**July 18, 2023 • 4:30 AM**

© 2023 All Rights are Reserved by HivePro



More at [www.hivepro.com](http://www.hivepro.com)