Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Adobe Addressed a Zero-day Vulnerability in ColdFusion 2021 and 2018

Date of Publication	Admiralty Code	TA Number
March 16, 2023	A1	TA2023138

Summary

First Seen: March 2023
Affected Product: Adobe ColdFusion
Impact: The vulnerabilities could potentially result in arbitrary code execution and memory leaks.

⚙ CVEs

CVE	NAME	PATCH	CISA
CVE-2023-26359	Adobe ColdFusion Improper Access Control Vulnerability	✓	✗
CVE-2023-26360*	Adobe ColdFusion Improper Access Control Vulnerability	✓	✓
CVE-2023-26361	Adobe ColdFusion Memory leak Vulnerability	✓	✗

Vulnerability Details

#1

Adobe has recently released security updates for ColdFusion 2021 and 2018 versions, addressing critical and important vulnerabilities that could potentially result in arbitrary code execution and memory leaks. It has come to the company's attention that the CVE-2023-26360 vulnerability has been exploited in a limited number of attacks targeting Adobe ColdFusion. This vulnerability can be abused remotely by unauthenticated attackers without user interaction, owing to an Improper Access Control weakness.

#2

While Adobe has provided updates to resolve the issue, unsupported versions of ColdFusion will not receive any security updates. The US Cybersecurity and Infrastructure Security Agency (CISA) has urged all US federal civilian executive branch agencies to secure their systems against potential attacks using the CVE-2023-26360 exploits by April 5, 2023. It is highly recommended for administrators to install the security updates and apply the security configuration settings outlined in the ColdFusion 2018 and ColdFusion 2021 lockdown guides.

* Represents zero-day vulnerability

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-26359	ColdFusion: 2016 update 15 and earlier versions ColdFusion: 2021 Update 5 and earlier versions	cpe:2.3:a:adobe:coldfusion:2021:Update 5:*:*:*:*:*:*	CWE-502
CVE-2023-26360*			CWE-284
CVE-2023-26361			CWE-22

Recommendations

Security Leaders
Asset and vulnerability management solutions should be implemented to ensure that all internet-accessible devices are secure, patched, updated, hardened, and monitored. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize the vulnerability, identify the impacted assets, and patch them through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.

- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' on the following pages.

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	TA0003 Persistence	TA0002 Execution	TA0040 Impact
T1588 Obtain Capabilities	T1203 Exploitation for Client Execution	T1588.005 Exploits	T1588.006 Vulnerabilities

Patch Details

ColdFusion 2018 update 15 and earlier versions to update 16
ColdFusion 2021 update 5 and earlier versions to update 6

https://coldfusion.adobe.com/2023/03/released-coldfusion-2021-and-2018-march-2023-security-updates/

References

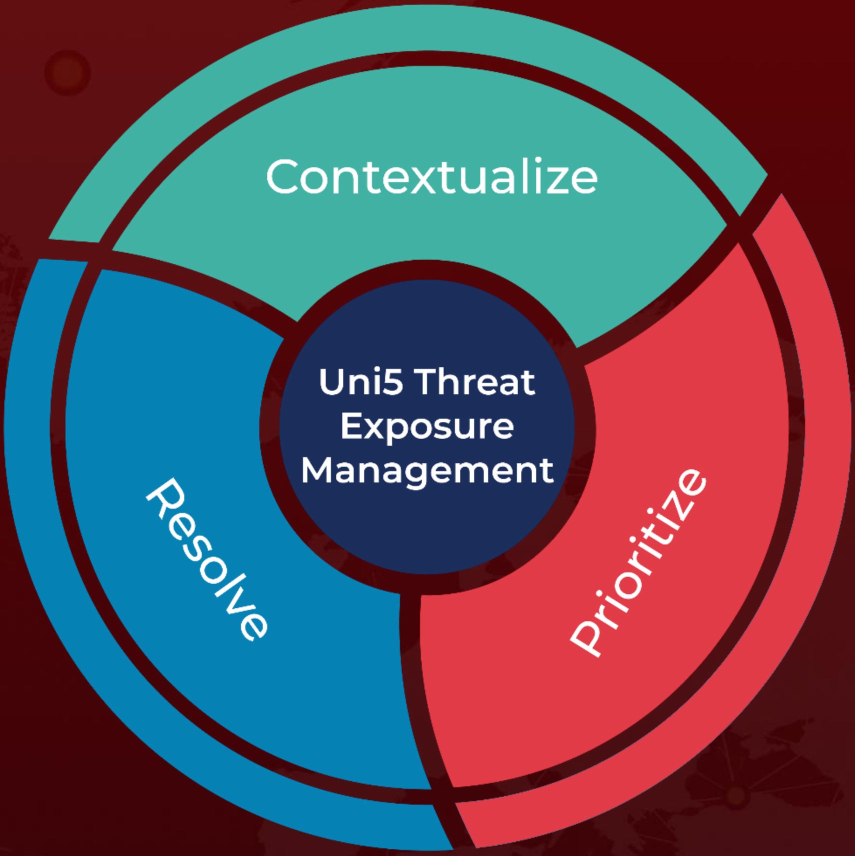
https://helpx.adobe.com/security/products/coldfusion/apsb23-25.html

https://www.cisa.gov/news-events/alerts/2023/03/15/cisa-adds-one-known-exploited-vulnerability-catalog

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

March 16, 2023 • 12:30 AM

More at www.hivepro.com