Hive Pro®

Threat Level

Red

CISA: AA23-339A

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

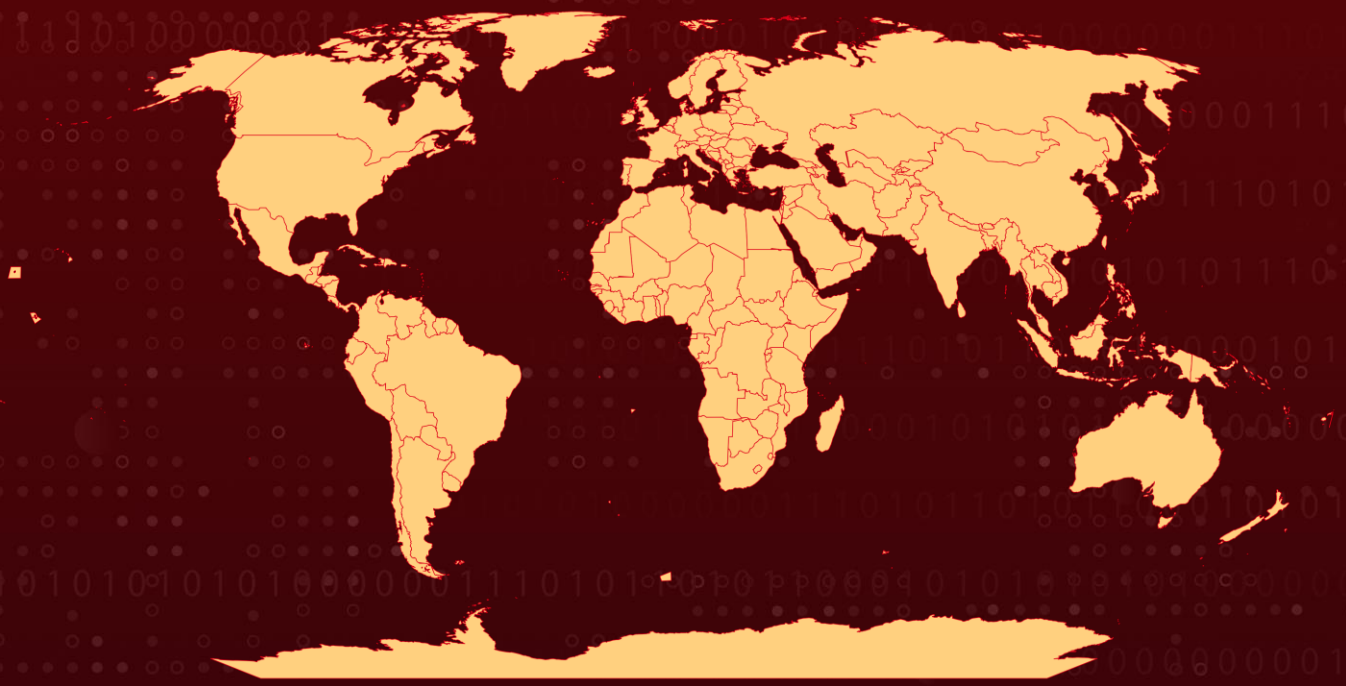
Adobe ColdFusion Vulnerability Leads to Federal Agency Breach

Date of Publication	Admiralty Code	TA Number
December 6, 2023	A1	TA2023489

Summary

Attack Began: June 2023
Attack Region: Worldwide
Threat Actor: Unknown
Targeted Industries: Government
Attack: Unidentified threat actors exploit Adobe ColdFusion vulnerability (CVE-2023-26360) on government servers, leading to potential unauthorized code execution. Incidents involve reconnaissance, data extraction attempts, and emphasize the importance of software updates.

Attack Regions



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-26360	Adobe ColdFusion Deserialization of Untrusted Data Vulnerability	Adobe ColdFusion	✓	✓	✓

Attack Details

#1 In June 2023, threat actors exploited a critical vulnerability in Adobe ColdFusion (CVE-2023-26360) to gain initial access to two agency systems at a Federal Civilian Executive Branch (FCEB) agency. This vulnerability affects Adobe ColdFusion versions 2018 Update 15 and earlier, as well as 2021 Update 5 and earlier. The vulnerability allows threat actors to execute arbitrary code on the vulnerable systems, which they used to drop malware, enumerate the network, and collect information about user accounts.

#2 In one incident, threat actors gaining initial access to a web server running an outdated version of Adobe ColdFusion. The attackers exploited the vulnerability, engaged in reconnaissance activities, and uploaded various malicious artifacts. Attempts were made to extract sensitive information from the server, including credentials from the ColdFusion configuration file.

#3 Incident two occurred on another public-facing web server running an outdated version of Adobe ColdFusion. Threat actors, using a malicious IP address, performed reconnaissance, collected information on administrative accounts, and deployed a remote access trojan (RAT) identified as a modified version of a publicly available web shell code. Efforts were made to exfiltrate registry files, but these actions were detected and blocked.Both incidents underline the importance of keeping software versions up to date to mitigate potential vulnerabilities.

Recommendations

Update Adobe ColdFusion: Ensure that Adobe ColdFusion is updated to the latest version. Apply patches and security updates provided by the software vendor to address known vulnerabilities. Regularly check for and apply new updates to stay protected against emerging threats.

Network Segmentation: Implement network segmentation to isolate critical systems and servers from public-facing environments. This can help contain the impact of a potential compromise and limit lateral movement within the network.

Access Controls: Review and enhance access controls for web servers and applications. Ensure that users and processes have the minimum necessary permissions required to perform their tasks. Regularly audit and update access control lists to align with the principle of least privilege.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0007 Discovery	TA0006 Credential Access
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0011 Command and Control
TA0043 Reconnaissance	T1059 Command and Scripting Interpreter	T1059.007 JavaScript	T1505.003 Web Shell
T1505 Server Software Component	T1484.001 Group Policy Modification	T1484 Domain Policy Modification	T1036.005 Match Legitimate Name or Location
T1036.008 Masquerade File Type	T1070.004 File Deletion	T1070 Indicator Removal	T1036 Masquerading
T1140 Deobfuscate/Decode Files or Information	T1564.001 Hidden Files and Directories	T1564 Hide Artifacts	T1003.001 LSASS Memory
T1003 OS Credential Dumping	T1003.002 Security Account Manager	T1016.001 Internet Connection Discovery	T1016 System Network Configuration Discovery
T1046 Network Service Discovery	T1082 System Information Discovery	T1083 File and Directory Discovery	T1087.001 Local Account
T1087 Account Discovery	T1087.002 Domain Account	T1482 Domain Trust Discovery	T1518 Software Discovery
T1071.001 Web Protocols	T1071 Application Layer Protocol	T1105 Ingress Tool Transfer	T1190 Exploit Public-Facing Application

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	a3acb9f79647f813671c1a21097a51836b0b95397ebc9cd178bc806e1773c864
SHA1	Be332b6e2e2ed9e1e57d8aafa0c00aa77d4b8656, B6818d2d5cbd902ce23461f24fc47e24937250e6
MD5	ba69669818ef9ccec174d647a8021a7b
IPv4	125.227.50[.]97, 158.101.73[.]241

Patch Details

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

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

References

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-339a

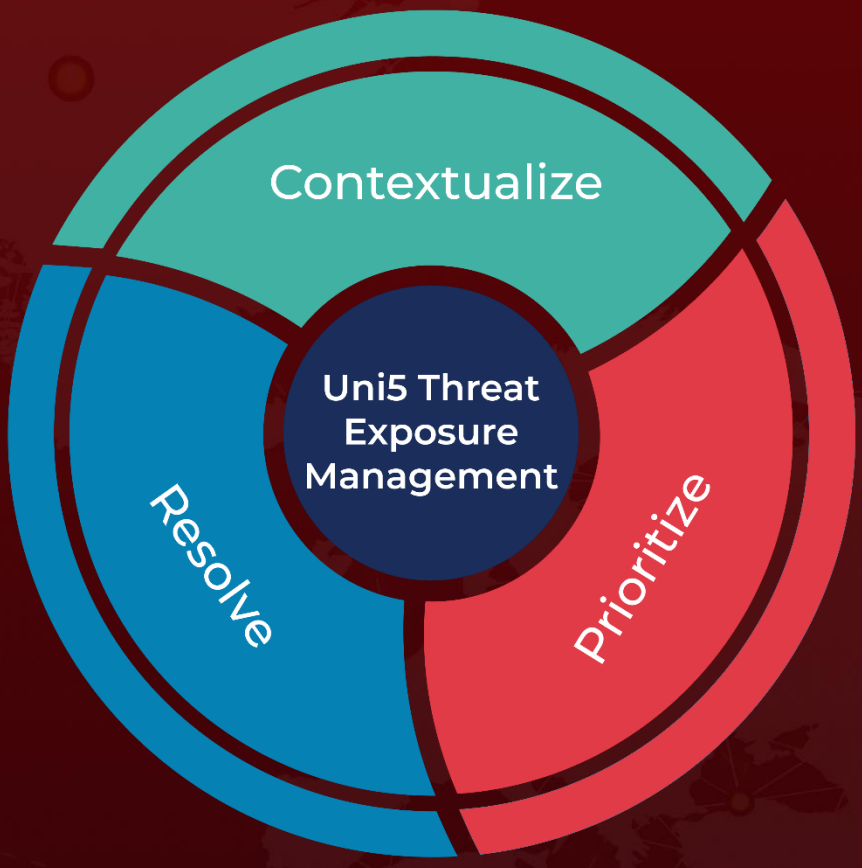
https://www.cisa.gov/news-events/alerts/2023/12/05/cisa-releases-advisory-threat-actors-exploiting-cve-2023-26360-vulnerability-adobe-coldfusion

https://www.hivepro.com/threat-advisory/adobe-addressed-a-zero-day-vulnerability-in-coldfusion-2021-and-2018/

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

December 6, 2023 . 4:30 AM

More at www.hivepro.com