CYBERSECURITY ADVISORY

Authored by:

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

TLP:CLEAR

Product ID: AA23-339A

December 5, 2023

Threat Actors Exploit Adobe ColdFusion CVE-2023-26360 for Initial Access to Government Servers

Actions to take today to mitigate malicious cyber activity:

- Prioritize remediating known exploited vulnerabilities.
- Employ proper network segmentation.
- Enable multifactor authentication (MFA) for all services to the extent possible, particularly for webmail, VPN, and accounts that access critical systems.

SUMMARY

The Cybersecurity and Infrastructure Security Agency (CISA) is releasing a Cybersecurity Advisory (CSA) in response to confirmed exploitation of CVE-2023-26360 by unidentified threat actors at a Federal Civilian Executive Branch (FCEB) agency. This vulnerability presents as an improper access control issue impacting Adobe ColdFusion versions 2018 Update 15 (and earlier) and 2021 Update 5 (and earlier). CVE-2023-26360 also affects ColdFusion 2016 and ColdFusion 11 installations; however, they are no longer supported since they reached end of life. Exploitation of this CVE can result in arbitrary code execution. Following the FCEB agency's investigation, analysis of network logs confirmed the compromise of at least two public-facing servers within the environment between June and July 2023.

This CSA provides network defenders with tactics, techniques, and procedures (TTPs), indicators of compromise (IOCs), and methods to detect and protect against similar exploitation.

For a downloadable copy of IOCs, see:

- AA23-339A (STIX XML, 24KB)
- AA23-339A (STIX JSON, 24KB)

TECHNICAL DETAILS

Note: This advisory uses the MITRE ATT&CK® for Enterprise framework, version 14. See the MITRE ATT&CK Tactics and Techniques section for tables mapped to the threat actors' activity.

To report suspicious or criminal activity related to information found in this Cybersecurity Advisory, contact CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282-0870. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

Overview

Adobe ColdFusion is a commercial application server used for rapid web-application development. ColdFusion supports proprietary markup languages for building web applications and integrates external components like databases and other third-party libraries. ColdFusion uses a proprietary language, ColdFusion Markup Language (CFML), for development but the application itself is built using JAVA.

In June 2023, through the exploitation of CVE-2023-26360, threat actors were able to establish an initial foothold on two agency systems in two separate instances. In both incidents, Microsoft Defender for Endpoint (MDE) alerted of the potential exploitation of an Adobe ColdFusion vulnerability on public-facing web servers in the agency's pre-production environment. Both servers were running outdated versions of software which are vulnerable to various CVEs. Additionally, various commands were initiated by the threat actors on the compromised web servers; the exploited vulnerability allowed the threat actors to drop malware using HTTP POST commands to the directory path associated with ColdFusion.

Analysis suggests that the malicious activity conducted by the threat actors was a reconnaissance effort to map the broader network. No evidence is available to confirm successful data exfiltration or lateral movement during either incident. **Note:** It is unknown if the same or different threat actors were behind each incident.

Incident 1

As early as June 26, 2023, threat actors obtained an initial foothold on a public-facing [T1190] web server running Adobe ColdFusion v2016.0.0.3 through exploitation of CVE-2023-26360. Threat actors successfully connected from malicious IP address `158.101.73[.]241`. **Disclaimer:** CISA recommends organizations investigate or vet this IP address prior to taking action, such as blocking. This IP resolves to a public cloud service provider and possibly hosts a large volume of legitimate traffic.

The agency's correlation of Internet Information Services (IIS) logs against open source[1] information indicates that the identified uniform resource identifier (URI) `/cf_scripts/scripts/ajax/ckeditor/plugins/filemanager/iedit.cfc` was used to exploit CVE-2023-26360. The agency removed the asset from the network within 24 hours of the MDE alert.

Threat actors started process enumeration to obtain currently running processes on the web server and performed a network connectivity check, likely to confirm their connection was successful. Following additional enumeration efforts to obtain information about the web server and its operating system [T1082], the threat actors checked for the presence of ColdFusion version 2018 [T1518]—previous checks were also conducted against version 2016.

Threat actors were observed traversing the filesystem [T1083] and uploading various artifacts to the web server [T1105], to include deleting the file `tat.cfm` [T1070.004]. **Note:** This file was deleted prior to the victim locating it on the host for analysis. Its characteristics and functionality are unknown. In addition:

- Certutil[2] was run against `conf.txt` [T1140] and decoded as a web shell (`config.jsp`) [T1505.003],[T1036.008]. `Conf.txt` was subsequently deleted, likely to evade detection. **Note:** Threat actors were only observed interacting with the `config.jsp` web shell from this point on.
- HTTP POST requests [T1071.001] were made to `config.cfm`, an expected configuration file in a standard installation of ColdFusion [T1036.005]. Code review of `config.cfm` indicated malicious code—intended to execute on versions of ColdFusion 9 or less—was inserted with the intent to extract username, password, and data source uniform resource locators (URLs). According to analysis, this code insertion could be used in future malicious activity by the threat actors (e.g., by using the valid credentials that were compromised). This file also contained code used to upload additional files by the threat actors; however, the agency was unable to identify the source of their origin.
- Threat actors attempted to run `attrib.exe` to hide the newly created `config.jsp` web shell [T1564.001]. Analysis of this phase found no indication of successful execution.
- A small subset of events generated from various ColdFusion application logs identified that `tat.cfm`, `config.jsp`, and `system.cfm` failed to execute on the host due to syntax errors.

Threat actors created various files (see Table 1 below) in the C:\IBM directory using the initialization process `coldfusion.exe`. None of these files were located on the server (possibly due to threat actor deletion) but are assessed as likely threat actor tools. Analysts assessed the C:\IBM directory as a staging folder to support threat actors' malicious operations.

Table 1: Threat Actor Tools

Disclaimer: Organizations are encouraged to investigate the use of these files for related signs of compromise prior to performing remediation actions. Two artifacts are legitimate Microsoft files; threat actors were observed using these files following initial compromise for intended malicious purposes.

File Name	Hash (SHA-1)	Description
eee.exe	b6818d2d5cbd902ce23461f24fc47e24937250e6	VirusTotal[3] flags this file as malicious. This was located in D:\$RECYCLE.BIN.
edge.exe	75a8ceded496269e9877c2d55f6ce13551d93ff4	The dynamic-link library (DLL) file `msedge.dll` attempted to execute via `edge.exe` but received an error. **Note:** This file is part of the official Microsoft Edge browser and is a cookie exporter.
fscan.exe	be332b6e2e2ed9e1e57d8aafa0c00aa77d4b8656	Analysis confirmed at least three subnets were scanned using `fscan.exe`, which was launched from the C:\IBM directory [T1046].
RC.exe	9126b8320d18a52b1315d5ada08e1c380d18806b	`RCDLL.dll` attempted to execute via `RC.exe` but received an error.

		Note: This file is part of the official Windows operating system and is called Microsoft Resource Compiler.

Note: The malicious code found on the system during this incident contained code that, when executed, would attempt to decrypt passwords for ColdFusion data sources. The seed value included in the code is a known value for ColdFusion version 8 or older—where the seed value was hard-coded. A threat actor who has control over the database server can use the values to decrypt the data source passwords in ColdFusion version 8 or older. The victim's servers were running a newer version at the time of compromise; thus, the malicious code failed to decrypt passwords using the default hard-coded seed value for the older versions.

Incident 2

As early as June 2, 2023, threat actors obtained an initial foothold on an additional public-facing web server running Adobe ColdFusion v2021.0.0.2 via malicious IP address `125.227.50[.]97` through exploitation of CVE-2023-26360. Threat actors further enumerated domain trusts to identify lateral movement opportunities [T1482] by using `nltest` commands. The threat actors also collected information about local [T1087.001] and domain [T1087.002] administrative user accounts while performing reconnaissance by using commands such as `localgroup`, `net user`, `net user /domain`, and `ID`. Host and network reconnaissance efforts were further conducted to discover network configuration, time logs, and query user information.

Threat actors were observed dropping the file `d.txt`—decoded as `d.jsp`—via POST command in addition to eight malicious artifacts (`hiddenfield.jsp`, `hiddenfield_jsp.class`, `hiddenfield_jsp.java`, `Connection.jsp`, `Connection_jsp.class`, `Connection_jsp.java`, `d_jsp.class`, and `d_jsp.java/`). According to open source information, `d.jsp` is a remote access trojan (RAT) that utilizes a JavaScript loader [T1059.007] to infect the device and requires communication with the actor-controlled server to perform actions.[4] The agency's analysis identified the trojan as a modified version of a publicly available web shell code.[5] After maintaining persistence, threat actors periodically tested network connectivity by pinging Google's domain name system (DNS) [T1016.001]. The threat actors conducted additional reconnaissance efforts via searching for the `.jsp` files that were uploaded.

Threat actors attempted to exfiltrate the (Registry) files `sam.zip`, `sec.zip`, `blank.jsp`, and `cf-bootstrap.jar`. Windows event logs identified the actors were not successful due to the malicious activity being detected and quarantined. An additional file (`sys.zip`) was created on the system; however, there were no indications of any attempt to exfiltrate it. Analysis identified these files resulted from executed save and compress data processes from the HKEY_LOCAL_MACHINE (HKLM) Registry key, as well as save security account manager (SAM) [T1003.002] information to .zip files. The SAM Registry file may allow for malicious actors to obtain usernames and reverse engineer passwords; however, no artifacts were available to confirm that the threat actors were successful in exfiltrating the SAM Registry hive.

Windows event logs show that a malicious file (`1.dat`) was detected and quarantined. Analysis determined this file was a local security authority subsystem service (LSASS) dump [T1003.001] file that contained user accounts—to include multiple disabled credentials—and Windows new technology LAN manager (NTLM) passwords. The accounts were found on multiple servers across the victim's network and were not successfully used for lateral movement.

As efforts for reconnaissance continued, the threat actors changed their approach to using security tools that were present on the victim server. `Esentutl.exe`[6] was used to attempt this registry dump. Attempts to download data from the threat actors' command and control (C2) server were also observed but blocked and logged by the victim server. Threat actors further attempted to access SYSVOL, which is used to deliver policy and logon scripts to domain members on an agency domain controller [T1484.001]. The attempt was unsuccessful. Had the attempt succeeded, the threat actors may have been able to change policies across compromised servers.[7]

Note: During this incident, analysis strongly suggests that the threat actors likely viewed the data contained in the ColdFusion seed.properties file via the web shell interface. The seed.properties file contains the seed value and encryption method used to encrypt passwords. The seed values can also be used to decrypt passwords. No malicious code was found on the victim system to indicate the threat actors attempted to decode any passwords using the values found in the seed.properties file. Versions of ColdFusion 9 or greater use the seed.properties file, which contains unique seed values that can only be used on a single server.

MITRE ATT&CK TACTICS AND TECHNIQUES

See Tables 2-9 for all referenced threat actor tactics and techniques for enterprise environments in this advisory. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping and CISA's Decider Tool.

Table 2: Initial Access

Technique Title	ID	Use
Exploit Public-Facing Application	T1190	Threat actors exploited two public-facing web servers running outdated versions of Adobe ColdFusion.

Table 3: Execution

Technique Title	ID	Use
Command and Scripting Interpreter: JavaScript	T1059.007	In correlation with open source information, analysis determined `d.jsp` is a RAT that utilizes a JavaScript loader to infect the device and requires communication with the actor-controlled server to perform actions.

Table 4: Persistence

Technique Title	ID	Use
Server Software Component: Web Shell	T1505.003	Threat actors uploaded various web shells to enable remote code execution and to execute commands on compromised web servers.

Table 5: Privilege Escalation

Technique Title	ID	Use
Domain Policy Modification: Group Policy Modification	T1484.001	Threat actors attempted to edit SYSVOL on an agency domain controller to change policies.

Table 6: Defense Evasion

Technique Title	ID	Use
Masquerading: Match Legitimate Name or Location	T1036.005	Threat actors inserted malicious code with the intent to extract username, password, and data source URLs into `config.cfm`—an expected configuration file in a standard installation of ColdFusion.
Masquerading: Masquerade File Type	T1036.008	Threat actors used the .txt file extension to disguise malware files.
Indicator Removal: File Deletion	T1070.004	Threat actors deleted files following upload to remove malicious indicators.
Deobfuscate/ Decode Files or Information	T1140	Threat actors used `certutil` to decode web shells hidden inside .txt files.
Hide Artifacts: Hidden Files and Directories	T1564.001	Threat actors attempted to run `attrib.exe` to hide the newly created `config.jsp` web shell.

Table 7: Credential Access

Technique Title	ID	Use
OS Credential Dumping: LSASS Memory	T1003.001	Threat actors attempted to harvest user account credentials through LSASS memory dumping.
OS Credential Dumping: Security Account Manager	T1003.002	Threat actors saved and compressed SAM information to .zip files.

Table 8: Discovery

Technique Title	ID	Use
System Network Configuration Discovery: Internet Connection Discovery	T1016.001	Threat actors periodically tested network connectivity by pinging Google's DNS.
Network Service Discovery	T1046	Threat actors scanned at least three subnets to gather network information using `fscan.exe`, to include administrative data for future exfiltration.
System Information Discovery	T1082	Threat actors collected information about the web server and its operating system.
File and Directory Discovery	T1083	Threat actors traversed and were able to search through folders on the victim's web server filesystem. Additional reconnaissance efforts were conducted via searching for the `.jsp` files that were uploaded.
Account Discovery: Local Account	T1087.001	Threat actors collected information about local user accounts.
Account Discovery: Domain Account	T1087.002	Threat actors collected information about domain users, including identification of domain admin accounts.
Domain Trust Discovery	T1482	Threat actors enumerated domain trusts to identify lateral movement opportunities.

Technique Title	ID	Use
Software Discovery	T1518	Following initial access and enumeration, threat actors checked for the presence of ColdFusion version 2018 on the victim web server.

Table 9: Command and Control

Technique Title	ID	Use
Application Layer Protocol: Web Protocols	T1071.001	Threat actors used HTTP POST requests to `config.cfm`, an expected configuration file in a standard installation of ColdFusion.
Ingress Tool Transfer	T1105	Threat actors were able to upload malicious artifacts to the victim web server.

MITIGATIONS

CISA recommends organizations implement the mitigations below to improve your organization's cybersecurity posture based on threat actor activity. These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. Visit CISA's Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections.

These mitigations apply to all critical infrastructure organizations and network defenders. CISA recommends that software manufacturers incorporate secure-by-design and -default principles and tactics into their software development practices, limiting the impact of threat actor techniques and strengthening the security posture for their customers. For more information on secure by design, see CISA's Secure by Design webpage.

Manage Vulnerabilities and Configurations

- **Upgrade all versions affected by this vulnerability.** Keep all software up to date and prioritize patching according to CISA's Known Exploited Vulnerabilities Catalog [1.E].
- **Prioritize remediation of vulnerabilities on internet-facing systems,** for example, by conducting continuous automated and/or routine vulnerability scans.
- **Prioritize secure-by-default configurations** such as eliminating default passwords, implementing single sign-on (SSO) technology via modern open standards. This also includes disabling default credentials.

Segment Networks

- **Employ proper network segmentation, such as a demilitarized zone (DMZ)** [2.F]. The end goal of a DMZ network is to allow an organization to access untrusted networks, such as the internet, while ensuring its private network or local area network (LAN) remains secure. Organizations typically store external-facing services and resources—as well as servers used for DNS, file transfer protocol (FTP), mail, proxy, voice over internet protocol (VoIP)—and web servers in the DMZ.
- **Use a firewall or web-application firewall (WAF) and enable logging** [2.G, 2.T] to prevent/detect potential exploitation attempts. Review ingress and egress firewall rules and block all unapproved protocols. Limit risky (but approved) protocols through rules.
- **Implement network segmentation to separate network segments based on role and functionality** [2.E]**.** Proper network segmentation significantly reduces the ability for threat actor lateral movement by controlling traffic flows between—and access to—various subnetworks. See CISA's Layering Network Security Through Segmentation infographic and the National Security Agency's (NSA's) Segment Networks and Deploy Application-Aware Defenses.
- **Deploy application-aware network defenses to block improperly formed traffic and restrict content,** according to policy and legal authorizations. Traditional intrusion detection systems (IDS) based on known-bad signatures are quickly decreasing in effectiveness due to encryption and obfuscation techniques. Threat actors hide malicious actions and remove data over common protocols, making the need for sophisticated, application-aware defensive mechanisms critical for modern network defenses.

Application Control

- **Enforce signed software execution policies.** Use a modern operating system that enforces signed software execution policies for scripts, executables, device drivers, and system firmware. Maintain a list of trusted certificates to prevent and detect the use and injection of illegitimate executables. Execution policies, when used in conjunction with a secure boot capability, can assure system integrity.
- **Application control should be used with signed software execution policies to provide greater control**. Allowing unsigned software enables threat actors to gain a foothold and establish persistence through embedded malicious code. See NSA's Enforce Signed Software Execution Policies.

Manage Accounts, Permissions, and Workstations

- **Require phishing-resistant multifactor authentication (MFA)** [2.H] for all services to the extent possible, particularly for webmail, VPN, and accounts that access critical systems.
- **Implement the principle of least privilege** to decrease threat actors' abilities to access key network resources.
- **Restrict file and directory permissions**. Use file system access controls to protect folders such as C:\Windows\System32.

- **Restrict NTLM authentication policy settings,** including incoming NTLM traffic from client computers, other member servers, or a domain controller.[8]

VALIDATE SECURITY CONTROLS

In addition to applying mitigations, CISA recommends exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. CISA recommends testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see Tables 2-9).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies' performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

CISA recommends continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

RESOURCES

- NIST: CVE-2023-26360
- CISA: KEV Catalog
- CISA, MITRE: Best Practices for MITRE ATT&CK Mapping
- CISA: Decider Tool
- CISA: Cross-Sector Cybersecurity Performance Goals
- CISA: Secure by Design and Default
- CISA: Layering Network Security Through Segmentation
- NSA: Segment Networks and Deploy Application-Aware Defenses
- NSA: Enforce Signed Software Execution Policies
- CISA: Implementing Phishing-Resistant MFA

REFERENCES

[1] Packet Storm Security: Adobe ColdFusion Unauthenticated Remote Code Execution
[2] MITRE: certutil
[3] VirusTotal: File - a3acb9f79647f813671c1a21097a51836b0b95397ebc9cd178bc806e1773c864
[4] Bleeping Computer: Stealthy New JavaScript Malware Infects Windows PCs with RATs
[5] GitHub: Tas9er/ByPassGodzilla
[6] MITRE: esentutl

[7] Microsoft: Active Directory - SYSVOL
[8] Microsoft: Restrict NTLM - Incoming NTLM Traffic

DISCLAIMER

The information in this report is being provided “as is” for informational purposes only. CISA does not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA.

VERSION HISTORY

December 5, 2023: Initial version.