FORTINET

OUTBREAK ALERTS

Adobe ColdFusion Access Control Bypass Attack

Critical-level detections in the wild

https://helpx.adobe.com/security/products/coldfusion/apsb23-52.html
CVEs: CVE-2023-26347,CVE-2023-38205,CVE-2023-29298,CVE-2023-38203

FortiGuards labs observed extremely widespread exploitation attempts relating to security bypass vulnerabilities in Adobe ColdFusion. Successful exploitation could result in access of the ColdFusion Administrator endpoints.

Background

Adobe ColdFusion is a commercial rapid web-application development computing platform to rapidly build, test and deploy web applications. Previously, in Aug 2023, we saw it being actively targeted by the attackers to exploit CVE-2023-26359. CVE-2023-26360 which lead to the release of an Outbreak Alert at that time, to read the full Outbreak visit:
https://www.fortiguard.com/outbreak-alert/adobe-coldfusion-code-execution

Latest Developments

January 9, 2024: FortiGuard Labs observed critical level of continued attacks on Adobe Coldfusion with IPS detections reaching upto 50,000+ unique detections. Users of Adobe ColdFusion are advised to apply patches as per vendor guidelines as soon as possible to mitigate any risk completely, if not already done.

January 8, 2024: CVE-2023-38203- Adobe ColdFusion Deserialization of Untrusted Data Vulnerability, was added to CISA KEV list and has been seen to be actively exploited.

November 28, 2023: CVE-2023-26347- Another Access Control Bypass vulnerability was announced and Adobe released patches for it.

https://helpx.adobe.com/ca/security/products/coldfusion/apsb23-52.html

July 20, 2023: Adobe ColdFusion vulnerabilities (CVE-2023-38205, CVE-2023-29298) were added to CISA's KEV catalog.

July 19, 2023: Adobe released security updates for ColdFusion versions 2023, 2021 and 2018 to fix (CVE-2023-38205).

At the time of the release, Adobe mentioned that CVE-2023-38205 has been exploited in the wild and has been seen in limited attacks. Please note, CVE-2023-38205 was released as a fix for incomplete patch for CVE-2023-29398.
https://helpx.adobe.com/security/products/coldfusion/apsb23-47.html

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

- Reconnaissance
- Weaponization
- **Delivery**

Vulnerability

Detects end-user devices running the vulnerable application.

FortiClient
DB 1.506

- **Exploitation**

IPS

Detects and blocks attack attempts leveraging the vulnerability

FortiADC *DB 26.680*
FortiGate *DB 26.680*
FortiNDR *DB 26.680*
FortiProxy *DB 26.680*
FortiSASE *DB 26.680*

Web App Security

Detects and blocks attack attempts leveraging the vulnerability

FortiADC
DB 1.00048

- Installation
- C2
- Action

DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

IOC

FortiAnalyzer
FortiSOCaaS
FortiSIEM

Outbreak Detection

FortiAnalyzer *DB 2.00034*
FortiSIEM *DB 603*

Threat Hunting

FortiAnalyzer
v6.4+

Playbook

FortiNDR Cloud
FortiSOAR
v7.4+

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

FortiXDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.

Incident Response
FortiRecon: ACI

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.

NSE Training
Response Readiness

End-User Training

Raise security awareness to your employees that are continuously being targeted by phishing, drive-by download and other forms of cyberattacks.

Security Awareness & Training

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.

Security Rating
FortiDAST

Vulnerability Management

Reduce the attack surface on software vulnerabilities via systematic and automated patching.

FortiClient

Business Reputation

Know attackers next move to protect against your business branding.

FortiRecon: EASM

Additional Resources

Bleeping Computer https://www.bleepingcomputer.com/news/security/adobe-fixes-patch-bypass-for-exploited-coldfusion-cve-2023-29298-flaw/

The Hacker News https://thehackernews.com/2023/07/adobe-rolls-out-new-patches-for.html

Learn more about FortiGuard Outbreak Alerts

FORTINET