



Adobe ColdFusion Deserialization of Untrusted Data Vulnerabilities

Exploited in the wild and actively targeted

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

CVEs: CVE-2023-26359, CVE-2023-26360

FortiGuard Labs continue to see cyber-attacks targeting to exploit the ColdFusion vulnerability CVE-2023-26360. Blocking over multiple hundreds of attacks over the last weeks.

Background

Adobe ColdFusion is a commercial rapid web-application and mobile applications development platform. Adobe ColdFusion is affected by Deserialization of Untrusted Data vulnerabilities (CVE-2023-26359, CVE-2023-26360) that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require any user interaction.

Announced

March 14, 2023: Adobe released the advisory and confirmed exploitation. "Adobe is aware that CVE-2023-26360 has been exploited in the wild in very limited attacks targeting Adobe ColdFusion."

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

March 15, 2023: FortiGuard Labs released Threat Signal (CVE-2023-26360)

<https://www.fortiguard.com/threat-signal-report/5063>

March 15, 2023: CISA added (CVE-2023-26360) to its known exploited catalog (KEV)

Latest Developments

Aug 21, 2023: CISA added CVE-2023-26359 to its known exploited list

FortiGuard customers remain protected by the IPS signature added for CVE-2023-26360 back in April 2023. However, we continue to see targeted attacks to exploit the vulnerability. IPS devices blocked over multiple hundred of attacks over the last month. FortiGuard Labs is investigating IPS protection for CVE-2023-26359 and will update this report once there is any new update.

FortiGuard Labs strongly advises to see vendor advisory and apply patches to Adobe Coldfusion if not already done.

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

PROTECT

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

Reconnaissance

Weaponization

Delivery

AV

Detects and blocks known malware targeting Adobe ColdFusion vulnerability (CVE-2023-26360, CVE-2023-26359)



FortiGate



FortiWeb



FortiSASE



FortiMail



FortiCASB



FortiCWP



FortiADC



FortiProxy

Vulnerability

Detects vulnerable instances of Adobe ColdFusion (CVE-2023-26359 CVE-2023-26360 CVE-2023-26361)



FortiClient

v1.525

AV (Pre-filter)

Detects and blocks known malware targeting Adobe ColdFusion vulnerability (CVE-2023-26360, CVE-2023-26359)



FortiSandbox



FortiNDR

Exploitation

IPS

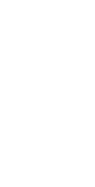
Detects and blocks attack attempts targeting Adobe ColdFusion vulnerability (CVE-2023-26360)



FortiGate



FortiSASE



FortiNDR



FortiADC



FortiProxy

DB 23.555

DB 23.555

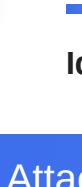
DB 23.555

DB 23.555

DB 23.555

Web App Security

Detects and blocks attack attempts targeting Adobe ColdFusion vulnerability (CVE-2023-26360)



FortiWeb

DB 0.00355

Installation

C2

Action

DETECT

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

Outbreak Detection



FortiClient



FortiAnalyzer

DB 1.00013 DB 2.00018

Threat Hunting

FortiAnalyzer

v6.4+

Content Update

FortiSIEM

DB 319

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

FortiXDR

FortiSASE

DB 23.555

DB 23.555

FortiNDR

FortiADC

FortiProxy

DB 23.555

DB 23.555

DB 23.555

Assisted Response Services

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

FortiResponse

FortiRecon.

DB 23.555

DB 23.555

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

DB 0.00355

DB 0.00355

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

Awareness

DB 319

DB 319

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

Rating

DB 23.555

DB 23.555

Business Reputation

Know attackers next move to protect against your business branding.

FortiRecon.

EASM

DB 319

DB 319

Additional Resources

Bleeping Computer

<https://www.bleepingcomputer.com/news/security/cisa-warns-of-adobe-coldfusion-hun-exploited-as-a-zero-day/>

HelpNet Security

<https://www.helpnetsecurity.com/2023/04/04/exploitation-cve-2023-26360-cve-2023-26359/>

Learn more about [FortiGuard Outbreak Alerts](#)