Adobe Fixed ColdFusion Flaw Listed as Under Active Exploit.

Severity: High

Date: 16th March 2023

Description

Adobe released security updates for ColdFusion versions 2021 and 2018 to resolve a critical flaw, tracked as CVE-2023-26360 (CVSS base score 8.6), that was exploited in very limited attacks.

This critical arbitrary code execution flaw (CVE-2023-26360) is due to an improper access control weakness, and it can be abused remotely by unauthenticated attackers in low-complexity attacks that don't require user interaction.

Background

Affected Adobe is aware that CVE-2023-26360 has been exploited in the wild in very limited attacks targeting adobe ColdFusion. The vulnerability is an improper access control that can allow a remote attacker to execute arbitrary code. The vulnerability could also lead to arbitrary file system read and memory leak.

The company also fixed a critical deserialization of untrusted data issue in adobe ColdFusion, tracked as CVE-2023-26359 (CVSS base score 9.8), that can lead to arbitrary code execution, also fixed a ColdFusion improper limitation of a pathname to a restricted directory ('Path Traversal'), tracked as CVE-2023-26361 (CVSS base score 4.9) that can lead to memory leak.

Recommendation

Advised to install the security patches as soon as possible and apply security configuration settings outlined in the ColdFusion 2018 and ColdFusion 2021 lockdown guides.

Reference Links

CISA warns of Adobe ColdFusion bug exploited as a zero-day (bleepingcomputer.com)

Adobe fixed Cold Fusion flaw listed as under active exploitSecurity Affairs