CERT-EU

Security Advisory 2023-046

Access Control Bypass Vulnerability in Adobe ColdFusion

July 12, 2023 — v1.0

TLP:CLEAR

Summary

Rapid7 discovered an access control bypass vulnerability in Adobe ColdFusion. This vulnerability allows an attacker to bypass access control restrictions by adding an additional forward slash to the requested URL. Adobe has released a fix for this vulnerability on July 11, 2023.

Technical Details

The vulnerability is caused by an issue in the `coldfusion.filter.IPFilterUtils` class. An HTTP request's URL path is compared to a list of sensitive paths, and if the request URL path starts with any of these sensitive paths, a further check is performed to verify if the request's external IP address is present in the allow list. If the request to a sensitive path is not from an allowed external IP address, an exception is raised resulting in the request being denied. However, this access check can be bypassed by inserting an additional character, specifically a forward slash, at the start of the URL path.

It should be emphasised that while the attacker can reach these resources, this does not automatically grant them the permissions to use these resources. Many of these resources will perform checks for authenticated sessions before initiating their actions. Regardless, the implications of an attacker gaining access to these resources include:

- The potential for an attacker to log into the ColdFusion Administrator, provided they have valid credentials.
- The possibility for an attacker to attempt brute-forcing credentials.
- The risk of an attacker leaking sensitive information.

Affected Products

The following versions of Adobe ColdFusion are affected:

- Adobe ColdFusion 2023
- Adobe ColdFusion 2021 Update 6 and below
- Adobe ColdFusion 2018 Update 16 and below

Recommendations

Adobe has released the following versions to remediate this issue:

- ColdFusion 2023 GA build
- ColdFusion 2021 Update 7
- ColdFusion 2018 Update 17

Users are advised to update to the latest version to mitigate this vulnerability.

References

[1] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29298