CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2019-006

Adobe ColdFusion
Critical Arbitrary Code Execution

March 7, 2019 — v1.0

TLP:WHITE

History:

- *7/03/2019 — v1.0 – Initial publication*

Summary

A critical vulnerability (CVE-2019-7816) [1, 2] in the web application development platform Adobe ColdFusion has been recently patched. The vulnerability allows attackers to execute arbitrary code bypassing a file upload restriction. Adobe released a Security Bulletin [3] that provides related information on the available patching of the affected versions.

Technical Details

The flaw allows a perpetrator to bypass file upload restrictions on the vulnerable server. A well-known attack method can be implemented by uploading malicious code to a web-accessible directory and then execute it on the targeted server.

The solution is to protect/filter file uploading and restrict permissions on executing code on the server [4]. Update of the ColdFusion installations is mandatory and of high priority according to Adobe [3].

Products Affected

The vulnerability affects ColdFusion 2018 update 2 and earlier, ColdFusion 2016 update 9 and earlier, as well as ColdFusion 11 update 17 and earlier versions.

Recommendations

It is highly recommended to update ColdFusion 2018 to update 3, ColdFusion 2016 to update 10 and ColdFusion 11 to update 18.

References

[1] https://threatpost.com/adobe-patches-critical-coldfusion-vulnerability-with-active-exploit/142391/

[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7816

[3] https://helpx.adobe.com/security/products/coldfusion/apsb19-14.html

[4] https://www.carehart.org/blog/client/index.cfm/2019/3/1/urgent_CF_security_update_Part_1