预警编号：YJ-2017026

恒安嘉新

关于 Adobe ColdFusion 存在反序列化

远程代码执行漏洞

安全预警通告

恒安嘉新（北京）科技股份公司

2017 年 10 月 18 日

1 漏洞描述

近期，互联网爆出 Adobe ColdFusion 反序列化漏洞（CVE-2017-11283），综合利用漏洞，攻击者成功利用漏洞可导致敏感信息泄露及远程代码执行。漏洞危害程度为高危(High)。

2 影响范围

1) ColdFusion 11 Update 12 及之前版本

2) ColdFusion （2016 release） Update 4 及之前版本

3 漏洞原理

ColdFusion，是 Adobe 旗下的一个动态 Web 服务器，其 CFML（ColdFusion Markup Language）是一种程序设计语言，类似现在的 JSP 里的 JSTL（JSP Standard Tag Lib），从 1995 年开始开发，其设计思想被一些人认为非常先进，被一些语言所借鉴。

ColdFusion 存在反序列化漏洞，其在开启“Remote Adobe LiveCycle Data Management access”功能的条件下会开启 rmi registery 服务，且会在本地监听 1099 端口。由于程序未对不可信的数据做校验就进行了反序列化的操作，攻击者可通过 RMI 协议向 Adobe ColdFusion 服务端发送精心构造的反序列化代码来触发漏洞实现远程代码执行，并且在返回数据包中泄漏 ColdFusion 路径以及 jar 包等敏感数据。

4 修复建议

目前，官方发布的安全更新，建议用户及时升级最新补丁：

1) ColdFusion 11 Update13:

http://helpx.adobe.com/coldfusion/kb/coldfusion-11-update-13.html

2) ColdFusion (2016 release) Update 5:

http://helpx.adobe.com/coldfusion/kb/coldfusion-2016-update-5.html

另，不能及时升级补丁的用户，建议可以采用如下临时解决方案：

检查 1099 端口是否开放，如果开放则存在安全隐患，请及时关闭“Remote Adobe LiveCycle DataManagement access”服务。