预警编号：YJ-2017033

恒安嘉新

关于 Apache Synapse 存在

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 12 月 11 日

1 漏洞描述

近日，Apache Synapse 发布了新版本修复的一个远程代码执行漏洞（CVE-2017-15708）。攻击者可利用上述漏洞通过注入特制的序列化对象的方式远程执行代码。漏洞危害程度为高危(High)。

2 影响范围

Apache Synapse 3.0.1 之前的所有版本

3 漏洞原理

Apache Synapse 是一个简单的、高质量开放源代码的替代方法，为实现 SOA 提供了一种途径，它可以公开现有的应用程序，而无需重新编写任何代码。

该漏洞源于 Apache Commons Collections 库包含“functor”包中的各个类可被序列化所致。攻击者可以通过注入特制的序列化对象，并在其类路径中包含 Apache Commons Collections 库，且不执行任何类型的输入验证，导致可远程执行代码。

4 修复建议

Apache Synapse 官方已经发布了最新的 3.0.1 版本修复该漏洞，强烈建议受影响的用户尽快升级到最新版本：http://synapse.apache.org/download/3.

0.1/download.cgi。