预警编号：YJ-2018017

恒安嘉新

关于 Apache Struts2 Commons FileUpload 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

2018 年 11 月 08 日

1 漏洞描述

近日,互联网爆出 Apache Struts2 Commons FileUpload 反序列化远程代码执行漏洞（CVE-2016-1000031）。攻击者利用该漏洞，可在未授权的情况下远程执行代码。该漏洞危害程度为高危(High)。目前，厂商已发布了漏洞修复补丁。

2 影响范围

受影响版本：

Struts 2.5.12 以下版本

3 漏洞原理

Struts2 是第二代基于 Model-View-Controller（MVC）模型的 java 企业级 web 应用框架，成为国内外较为流行的容器软件中间件。

2018 年 11 月 5 日，Apache Strust2 发布最新安全公告，Apache Struts2 存在远程代码执行的高危漏洞（CVE-2016-1000031），该漏洞由 Tenable 研究团队发现。此漏洞为 FileUpload 库中的一个高危漏洞，这个库作为 Apache Struts 2 的一部分，被用作文件上传的默认机制。攻击者可以在未经授权的情况下，执行任意代码并可获取目标系统的所有权限。

4 修复建议

目前，厂商已发布了最新版本修复了漏洞，具体修复建议如下：

建议及时更新至最新版本：Struts 2.5.12 及以上版本，包括 Commons FileUpload 库的修补版本 1.3.3。

附：参考链接：

https://issues.apache.org/jira/browse/FILEUPLOAD-279