|  |
| --- |
| 【文档编号：2019031301】 |
| 四川省生态环境厅安全报告宜宾市生态环境局Java目录穿越漏洞安全事件分析 |
| 二〇一九年三月 |

**目 录**

[1 基本信息：宜宾市生态环境局 1](#_Toc3795280)

[2 事件综述 1](#_Toc3795281)

[2.1 事件概述 1](#_Toc3795282)

[2.2 事件定位分析 1](#_Toc3795283)

[3 建议与措施 3](#_Toc3795284)

# 基本信息：宜宾市生态环境局

|  |  |  |  |
| --- | --- | --- | --- |
| **资产IP** | 10.0.8.20 | **隶属** | 宜宾市生态环境局 |
| **发现时间** | 2019年3月11日 | **处理期限** |  | **漏洞类型** | 文件信息泄露 |
| **漏洞名称** | Java目录穿越漏洞 | **漏洞级别** |  ☑高危 □中危 □低危 |
| **危害表象** | □网络中断  ☑系统瘫痪  ☑数据毁坏  ☑数据泄密  ☑其它危害 |

# 事件综述

## 事件概述

通过AiLPHA大数据平台分析发现，2019年3月11日至2019年3月15日中宜宾市生态环境局IP：10.0.8.20被检测到有Java目录穿越漏洞，在此期间不间断地被攻击者利用此漏洞进行攻击，共计69条。



## 事件定位分析

Java穿越目录漏洞是目录遍历漏洞的一种。攻击人员通过目录遍历攻击可以获取系统文件及服务器的配置文件等等。一般来说，他们利用服务器API、文件标准权限进行攻击。如果web设计者设计的web内容没有恰当的访问控制，允许http遍历，攻击者就可以访问受限的目录，并可以在web根目录以外执行命令。

 通过平台检测到数据请求包（HTTP请求头）直接访问：125.64.218.67:81/AutoMonitorWebSite/Modules/WEB-INF/flex/services-config.xml，可以直接访问的看到Flex的配置文件service-config.xml。



通过使用Chrome浏览器（Firefox浏览器需要配置）访问后，页面响应回显flex框架的配置文件内容（service-config.xml）。



 通过沟通得知，部分功能确实使用的是Flex框架二次开发，使用的web服务器是tomcat。目前看来Flex框架本身出现框架的配置问题较少，推测应当是tomcat服务器配置问题。

# 建议与措施

1. 查看web log，如果发现有未授权用户访问越级目录，说明有目录便利漏洞。
2. 对该web服务器的配置进行调整：设置访问敏感信息文件的用户权限，仅供管理员访问；禁止使用特殊符号，如“…/“进行目录遍历。
3. 对网站框架配置文件设定隐藏不可见属性，禁止直接访问。