|  |
| --- |
| 【文档编号：2020021101】 |
| 四川省生态环境厅安全报告  广元市生态环境局  Java目录穿越安全事件 |
| 二〇二〇年二月 |

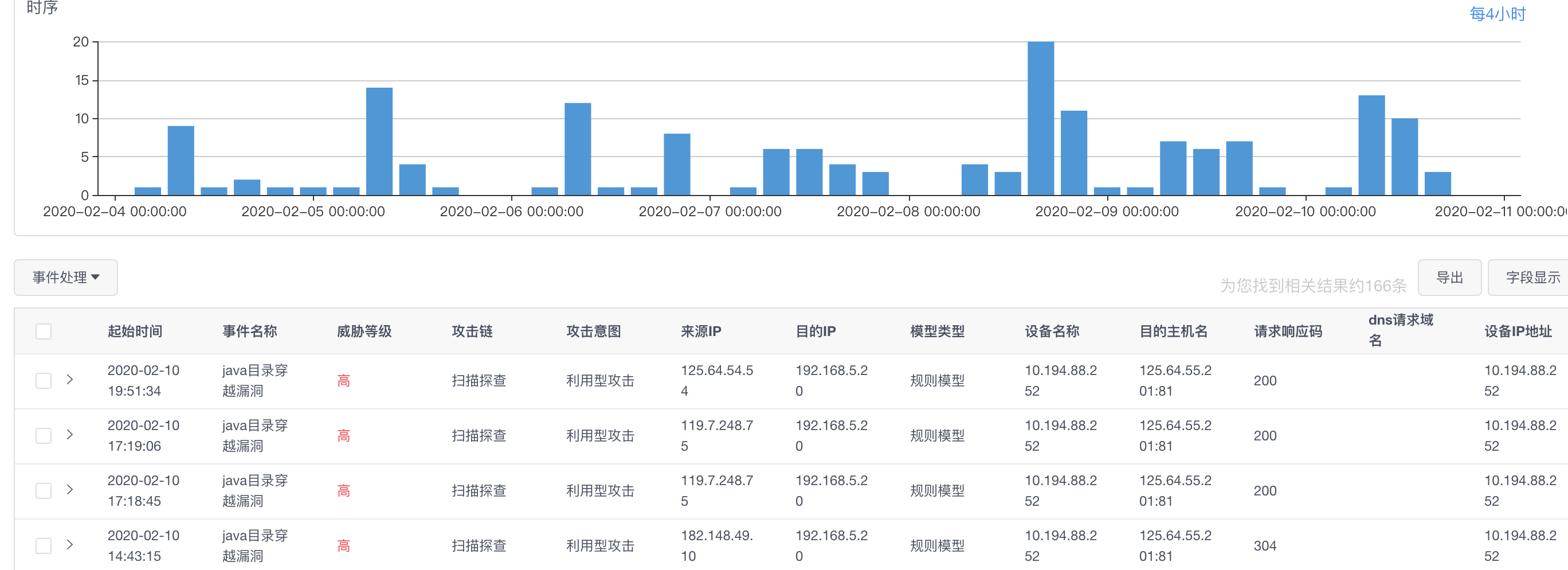
# 基本信息

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **资产IP** | 192.168.5.20 | | | **隶属** | 广元市生态环境局 |
| **发现时间** | 2020年2月11日 | **处理期限** |  | **事件类型** | 利用型攻击 |
| **事件名称** | java目录穿越漏洞 | | **事件级别** | □I级 □II级 ☑III级别 □IV级 | |
| **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，2020年2月4日-2020年2月11日，发现java目录穿越漏洞攻击共计166条，请求响应码200和304.





## 事件定位分析

外部攻击IP（判断为动态IP）：

119.7.248.75

182.148.49.10

222.213.168.122

117.173.124.66

118.121.117.92

139.202.59.248

119.7.254.190

125.64.55.249

175.153.168.12

171.91.253.64

175.153.160.5

119.5.208.97

221.236.208.58

175.153.160.3

175.153.160.4

113.200.204.106

171.216.125.94

175.153.160.10

123.138.232.164

123.139.80.240

175.153.168.16

222.211.1.228

221.236.208.193

183.227.240.36

175.153.168.3

123.138.233.19

123.139.86.214

175.153.160.11

118.121.243.244

118.125.121.169

171.91.243.234

171.216.122.180

222.215.214.57

221.182.123.87

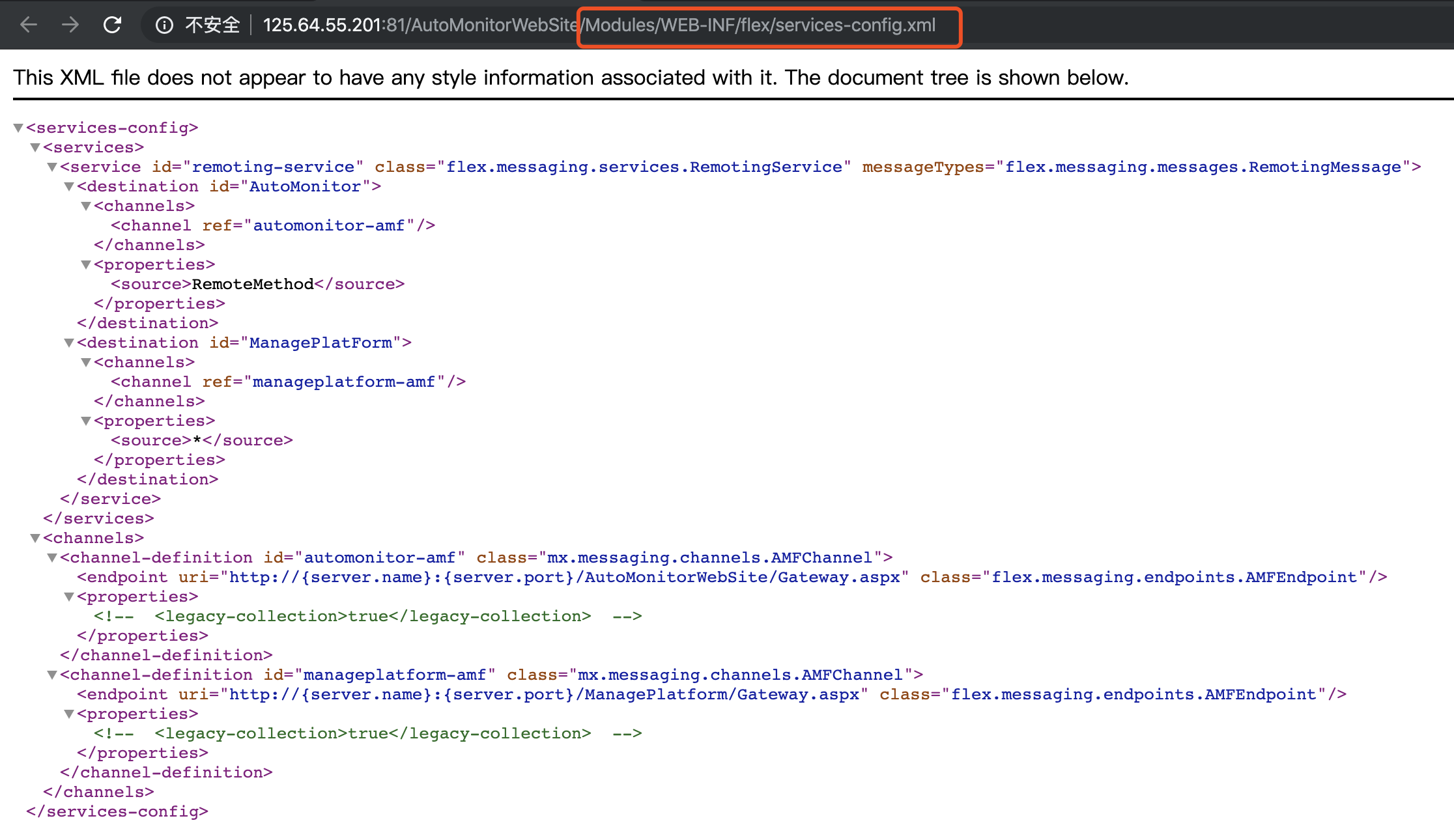
221.10.191.80

112.18.21.200

向广元市生态环境局IP：192.168.5.20的81端口发送Get请求。



已验证漏洞存在：



# 建议与措施

1、数据过滤，对网站用户提交过来的文件名进行硬编码或者统一编码，对文件后缀进行白名单控制，对包含了恶意的符号或者空字节进行拒绝。

2、Web应用程序可以使用chrooted环境访问包含被访问文件的目录，或者使用绝对路径+参数来控制访问目录，使其即使是越权或者跨越目录也是在指定的目录下。