New issue

Jump to bottom

There is a SSRF vulnerability via /publiccms/admin/ueditor #51

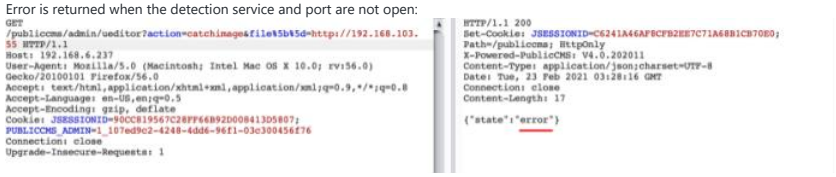
Closed seedis opened this issue on Feb 23, 2021 · 1 comment

seedis commented on Feb 23, 2021

Hello,I found a SSRF in the lastest version of PublicCMS-V4.0.202011.b

The vulnerability is triggered by visiting the following address after logging in the management background
http://192.168.6.237:8081/publiccms/admin/ueditor?action=catchimage&file%5b%5d=http://192.168.103.3
http://192.168.6.237:8081/publiccms/admin/ueditor?action=catchimage&file%5B%5D=https://www.baidu.com

The "file[]" parameter has a loophole, and the IP and domain names that access is not restricted, resulting in an SSRF loophole.
Error is returned when the detection service and port are not open:



Return success when detecting service and port opening:

Attackers can use this vulnerability to scan the internal network for open hosts and ports, and attack applications with vulnerabilities in the internal network, such as redis, struts2, etc., and further gain control of the server system.

PublicCMS is a useful development cms, I think we need to pay attention to and fix this security issue， looking forward to your reply.

sanluan commented on Feb 23, 2021 • edited Owner

对于已经拥有管理员权限的用户 想要做到这种攻击或者试探是很容易的 比如在模板中编写 ${getHtml('http://127.0.0.1:8080/')} ，就可以直接输出请求结果，这个功能可以方便的调用内网系统数据展示到外网中，和您的issues中图片抓取一样是非常实用的功能，很多场景也一样会涉及到内网图片的抓取，再加上还可以利用重定向的方式攻击，想要当作漏洞使用规则封堵这种行为尤其是对于开放型产品来说 很困难
不过您提供的这个漏洞我们打算用判断抓取的内容是否为图片的方式进行修复
目前cms中已经内置的解决方案是部署时配置代理，cms.proxy.enable=true,将所有这种危险的请求都控制在一个做了充分防火墙规则的孤立代理服务器上

sanluan added a commit that referenced this issue on Feb 23, 2021

https://github.com/sanluan/PublicCMS/issues/51 0f4c487

sanluan closed this as completed on Oct 28, 2021

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants