海思 1G无频 - Bug #3482

【Web安全扫描】 8080页面扫描有 909、10932漏洞

05/15/2025 14:45 - 邹迎春

Status:	Closed	**Start date:**	05/15/2025
Priority:	Normal	**Due date:**	
Assignee:	邹迎春	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:		**Spent time:**	0.00 hour
测试版本 **:**	emei_V1.0.2_ker_fs_53f245d4.bin	复现概率 **:**	100%

Description

【操作路径】:
步骤1: 使用扫描工具连接单板的LAN侧进行安全扫描;
步骤2: 设定认证账号为useradmin，进入到普通用户配置界面，测试是否有漏洞;
步骤3: 设定认证账号为telecomadmin，进入到管理界面，测试是否有漏洞;
步骤4: 分析扫描结果,对告警的各类问题进行分析。
【实际结果】:
8080页面扫描有909、10932漏洞，详请查阅附件
【预期结果】
扫描结果中，Critical、High、Medium、Low中的如下内容不被视作网关安全问题（Info 和BP非问题）：
中间件页面端口（80）：
Internal IP Disclosure（3508）
Cross-Site Scripting (5649)
Logins Sent Over Unencrypted Connection (4722)
Unencrypted Login Form (10595)
Possible Server Path Disclosure (unix) (810)
CGI and Scripting-Related Directories (10212)
Admin Section Must Require Authentication (4721)
Missing Content-Type Header (11308)
Browser Mime Sniffing is not disabled (11309)
Cross-Frame Scripting (11293)
Critical和High:Session Fixation (11201)
Password in Query or Cookie Data (10167)
"Admin" Directory (10810)
Server Error Response (10932)
Password Field Auto Complete Active (11276)
JSON Hijacking Possible (10731)
网关页面端口（8080）：
Internal IP Disclosure（3508）
Critical和High:Session Fixation (11201)
Password in Query or Cookie Data (10167)
Cross-Frame Scripting (11293)
Medium和Low: User Data in Query or Cookie (10965)
CGI and Scripting-Related Directories (10212)
Common Web Site Structure Directories (10214)

History

#1 - 05/15/2025 14:46 - 邹迎春

- Description updated

#2 - 05/20/2025 17:23 - 良缘 彭

- Status changed from New to Feedback

- Assignee changed from 良缘 彭 *to* 邹迎春

可能的文件上次功能（909）
网关需要有升级功能，上传文件是不可能避免的

服务器响应（10932）

这些url的响应是400 Bad Request，这个不能被看做问题

#3 - 05/21/2025 16:03 - 琪董

- File 0521-8080.pdf added

- Status changed from Feedback to Closed

新版本未扫描出（909），服务器响应（10932）这些url的响应是400 Bad Request，这个不能被看做问题
验证版本emei_default_ker_fs_fwk_819f8a64.bin

Files

telenetadmin1.pdf	298 KB	05/15/2025	邹迎春
0521-8080.pdf	289 KB	05/21/2025	琪董