Web 应用程序报告

该报告包含有关 web 应用程序的重要安全信息。

安全报告

该报告由 HCL AppScan Standard 创建 10.0.0, 规则： 0
扫描开始时间： 2025/4/1 9:18:44

目录

- 将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头
- 将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头
- 请勿接受在查询字符串中发送的主体参数
- 为 Web 服务器或 Web 应用程序下载相关的安全补丁

咨询

- BEA WebLogic URL 欺骗目录列表
- “Content-Security-Policy”头缺失或不安全
- “X-Content-Type-Options”头缺失或不安全
- “X-XSS-Protection”报头缺失或不安全
- 查询中接受的主体参数
- HTML 注释敏感信息泄露
- 发现可能的服务器路径泄露模式
- 发现内部 IP 泄露模式

应用程序数据

- cookie
- JavaScript
- 参数
- 注释
- 已访问的 URL
- 失败的请求
- 已过滤的 URL

介绍

该报告包含由 HCL AppScan Standard 执行的 Web 应用程序安全性扫描的结果。

中等严重性问题：	6
低严重性问题：	16
参考严重性问题：	3
报告中包含的严重性问题总数：	25
扫描中发现的严重性问题总数：	25

常规信息

扫描文件名称：	teleuseradmin
扫描开始时间：	2025/4/1 9:18:44
测试策略：	Default

主机	192.168.1.1
端口	80
操作系统：	未知
Web 服务器：	未知
应用程序服务器：	任何

主机	192.168.1.1
端口	8080
操作系统：	未知
Web 服务器：	未知
应用程序服务器：	任何

登陆设置

登陆方法：	记录的登录
并发登陆：	已启用
会话中检测：	已启用

会话中模式：

跟踪或会话 ID cookie：

跟踪或会话 ID 参数：

登陆序列：

摘要

问题类型 8

TOC

	问题类型	问题的数量
中	BEA WebLogic URL 欺骗目录列表	6
低	“Content-Security-Policy”头缺失或不安全	5
低	“X-Content-Type-Options”头缺失或不安全	5
低	“X-XSS-Protection”头缺失或不安全	5
低	查询中接受的主体参数	1
参	HTML 注释敏感信息泄露	1
参	发现可能的服务器路径泄露模式	1
参	发现内部 IP 泄露模式	1

有漏洞的 URL 15

TOC

	URL	问题的数量
中	http://192.168.1.1/luci-static/	1
中	http://192.168.1.1/luci-static/resources/	1
中	http://192.168.1.1/luci-static/resources/css/	1
中	http://192.168.1.1/luci-static/resources/image/	1
中	http://192.168.1.1/luci-static/resources/image/login/	1
中	http://192.168.1.1/luci-static/resources/js/	1
低	http://192.168.1.1/	3
低	http://192.168.1.1/luci-static/resources/js/util.js	3
低	http://192.168.1.1:8080/js/aes_1.js	3
低	http://192.168.1.1:8080/js/common.js	3
低	http://192.168.1.1:8080/maintain	3
低	http://192.168.1.1:8080/boaform/web_login_exe.cgi	1
参	http://192.168.1.1/cgi-bin/luci	1
参	http://192.168.1.1:8080/js/jquery.js	1

参	http://192.168.1.1:8080/login.html	1	

修订建议 8

TOC

	修复任务	问题的数量
中	安装 WebLogic 的最新版本和补丁	6
低	除去 HTML 注释中的敏感信息	1
低	除去 Web 站点中的内部 IP 地址	1
低	将服务器配置为使用安全策略的“Content-Security-Policy”头	5
低	将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头	5
低	将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头	5
低	请勿接受在查询字符串中发送的主体参数	1
低	为 Web 服务器或 Web 应用程序下载相关的安全补丁	1

安全风险 4

TOC

	风险	问题的数量
中	可能会查看和下载特定 Web 应用程序虚拟目录的内容，其中可能包含受限文件	6
低	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置	18
低	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息	16
参	可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息	1

原因 4

TOC

	原因	问题的数量
中	未安装第三方产品的最新补丁或最新修订程序	6
低	Web 应用程序编程或配置不安全	17
参	程序员在 Web 页面上留下调试信息	1
参	未安装第三方产品的最新补丁或最新修补程序	1

WASC 威胁分类

TOC

威胁	问题的数量
目录索引	6
信息泄露	19

按问题类型分类的问题

中 BEA WebLogic URL 欺骗目录列表 6 TOC

问题 1 / 6 TOC

BEA WebLogic URL 欺骗目录列表

严重性：	中
CVSS 分数：	6.4
URL：	http://192.168.1.1/luci-static/resources/image/
实体：	image/ (Page)
风险：	可能会查看和下载特定 Web 应用程序虚拟目录的内容，其中可能包含受限文件
原因：	未安装第三方产品的最新补丁或最新修订程序
固定值：	安装 WebLogic 的最新版本和补丁

差异： **方法** 从以下位置进行控制： `HEAD` 至： `GET`
路径 从以下位置进行控制： `/luci-static/resources/image/favicon.ico` 至： `/luci-static/resources/image/%2E/`

推理： 响应包含目录的内容（目录列表）。这表示服务器允许列示目录（通常不推荐此做法）。

测试请求和响应：

```
GET /luci-static/resources/image/%2E/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1/cgi-bin/luci
Connection: Keep-Alive
Host: 192.168.1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Transfer-Encoding: chunked
Connection: Keep-Alive
Keep-Alive: timeout=20
Date: Tue, 01 Apr 2025 01:22:06 GMT
Content-Type: text/html

<html><head><title>Index of /luci-static/resources/image/</title></head><body><h1>Index of /luci-
static/resources/image/</h1><hr /><ol><li><strong><a href='/luci-static/resources/image/../'>..
```

```
</a>/</strong><br /><small>modified: Sat, 22 Jun 2024 08:13:57 GMT<br />directory - 0.17 kbyte<br
/><br /></small></li><li><strong><a href='/luci-static/resources/image/home/'>home</a>/</strong>
<br /><small>modified: Sat, 22 Jun 2024 08:13:57 GMT<br />directory - 1.03 kbyte<br /><br />
</small></li><li><strong><a href='/luci-static/resources/image/login/'>login</a>/</strong><br />
<small>modified: Sat, 22 Jun 2024 08:13:57 GMT<br />directory - 0.34 kbyte<br /><br /></small>
</li><li><strong><a href='/luci-static/resources/image/Storage-LocalIco.png'>Storage-
LocalIco.png</a></strong><br /><small>modified: Fri, 13 Nov 2020 07:23:58 GMT<br />image/png -
1.99 kbyte<br /><br /></small></li><li><strong><a href='/luci-
static/resources/image/action_bg.png'>action_bg.png</a></strong><br /><small>modified: Fri, 13
Nov 2020 07:23:54 GMT<br />image/png - 2.35 kbyte<br /><br /></small></li><li><strong><a
href='/luci-static/resources/image/alert.png'>alert.png</a></strong><br /><small>modified: Fri,
13 Nov 2020 07:23:54 GMT<br />image/png - 1.62 kbyte<br /><br /></small></li><li><strong><a
href='/luci-static/resources/image/android.png'>android.png</a></strong><br /><small>modified:
Fri, 13 Nov 2020 07:23:58 GMT<br />image/png - 17.98 kbyte<br /><br /></small></li><li><strong><a
href='/luci-static/resources/image/androidapp.png'>androidapp.png</a></strong><br />
<small>modified: Fri, 13 Nov 2020 07:23:54 GMT<br />image/png - 1.92 kbyte<br /><br /></small>
</li><li><strong><a href='/luci-static/resources/image/app-code.png'>app-code.png</a></strong><br
/><small>modified: Fri, 13 Nov 2020 07:23:58 GMT<br />image/png - 1.06 kbyte<br /><br /></small>
</li><li><strong><a href='/luci-static/resources/image/appdownload.png'>appdownload.png</a>
</strong><br /><small>modified: Fri, 13 Nov 2020 07:23:54 GMT<br />image/png - 23.93 kbyte<br />
<br /></small></li><li><strong><a href='/luci-static/resources/image/audio.png'>audio.png</a>
</strong><br /><small>modified: Fri, 13 Nov 2020 07:23:51 GMT<br />image/png - 19.27 kbyte<br />
<br /></small></li><li><strong><a href='/luci-
static/resources/image/chinatelecom.png'>chinatelecom.png</a></strong><br /><small>modified: Fri,
13 Nov 2020 07:23:58 GMT<br />image/png - 1.18 kbyte<br /><br /></small></li><li><strong><a
href='/luci-static/resources/image/choose.png'>choose.png</a></strong><br /><small>modified: Fri,
13 Nov 2020 07:23:54 GMT<br />image/png - 1.02 kbyte<br /><br /></small></li><li><strong><a
href='/luci-static/resources/image/copyright_logo.png'>copyright_logo.png</a></strong><br />
<small>modified: Fri, 13 Nov 2020 07:23:58 GMT<br />image/png - 0.41 kbyte<br /><br /></small>
</li><li><strong><a href='/luci-static/resources/image/eye.png'>eye.png</a></strong><br />
<small>modified: Fri, 13 Nov 2020 07:23:54 GMT<br />image/png - 1.38 kbyte<br /><br /></small>
</li><li><strong><a href='/luci-static/resources/image/eye_close.png'>eye_close.png</a></strong>
<br /><small>modified: Fri, 13 Nov 2020 07:23:54 GMT<br />image/png - 1.45 kbyte<br /><br />
</small></li><li><strong><a href='/luci-
static/resources/image/eye_close_focus.png'>eye_close_focus.png</a></strong><br />
<small>modified: Fri, 13 Nov 2020 07:23:58 GMT<br />image/png - 1.49 kbyte<br /><br /></small>
</li><li><strong><a href='/luci-static/resources/image/favicon.ico'>favicon.ico</a></strong><br
/><small>modified: Fri, 13 Nov 2020 07:23:54 GMT<br />application/octet-stream - 4.19 kbyte<br />
<br /></small></li><li><strong><a href='/luci-static/resources/image/file.png'>file.png</a>
</strong><br /><small>modified: Fri, 13 Nov 2020 07:23:54 GMT<br />image/png - 18.87 kbyte<br />
<br /></small></li><li><strong><a href='/luci-
static/resources/image/first_menu_more_bg.png'>first_menu_more_bg.png</a></strong><br />
<small>modified: Fri, 13 Nov 2020 07:23:58 GMT<br />image/png - 1.09 kbyte<br /><br /></small>
</li><li><strong><a href='/luci-
static/resources/image/first_menu_primary_bg.png'>first_menu_primary_bg.png</a></strong><br />
<small>modified: Fri, 13 Nov 2020 07:23:58 GMT<br />image/png - 1.08 kbyte<br /><br /></small>
</li><li><strong><a href='/luci-static/resources/image/folder.png'>folder.png</a></strong><br />
<small>modified: Fri, 13
...
...
...
```

问题 2 / 6

TOC

BEA WebLogic URL 欺骗目录列表

严重性：	中
CVSS 分数：	6.4
URL：	http://192.168.1.1/luci-static/resources/css/
实体：	css/ (Page)
风险：	可能会查看和下载特定 Web 应用程序虚拟目录的内容，其中可能包含受限文件
原因：	未安装第三方产品的最新补丁或最新修订程序
固定值：	安装 WebLogic 的最新版本和补丁

差异： **方法** 从以下位置进行控制： `HEAD` 至： `GET`
路径 从以下位置进行控制： `/luci-static/resources/css/login.css` 至： `/luci-static/resources/css/%2E/`

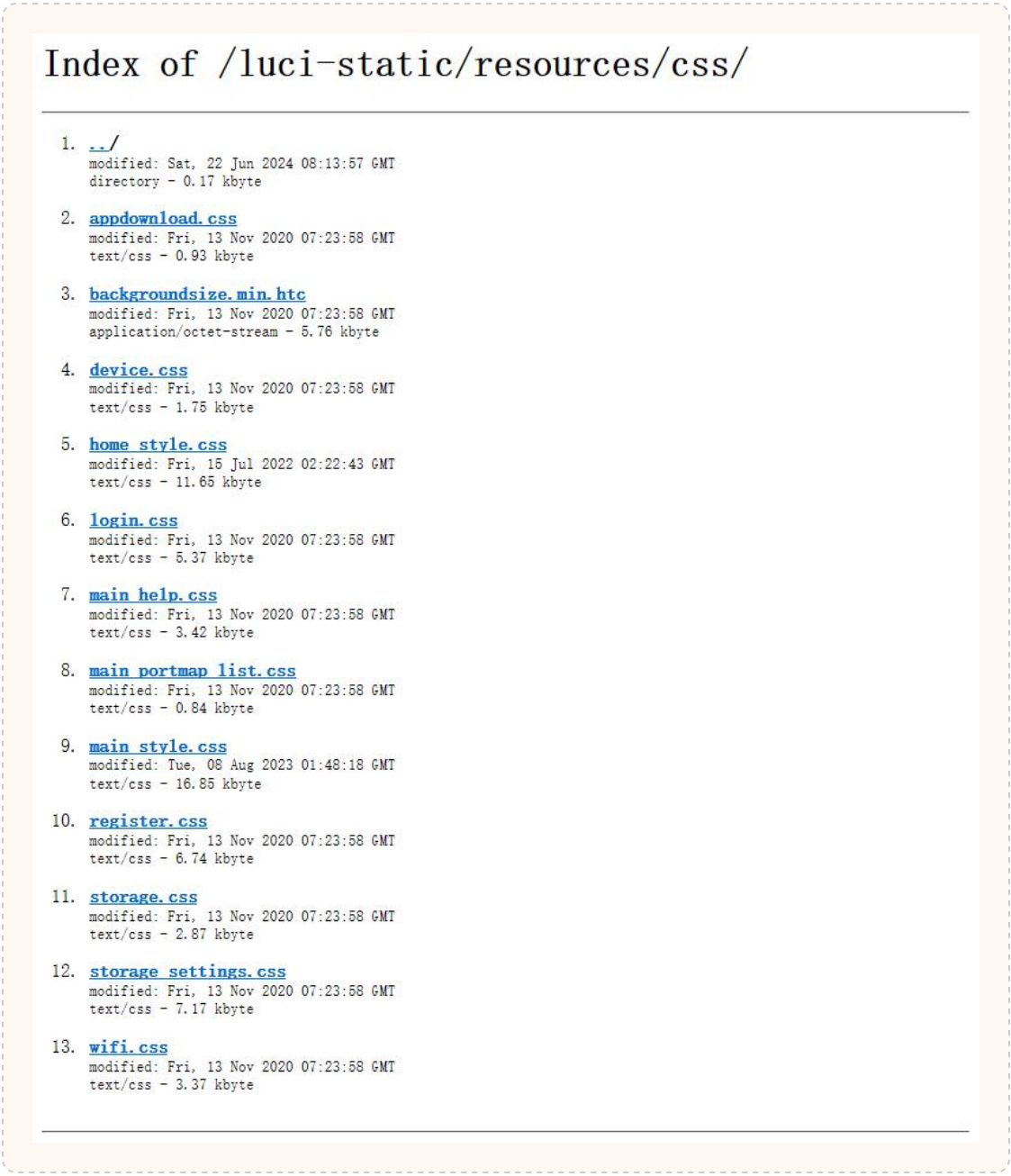
推理： 响应包含目录的内容（目录列表）。这表示服务器允许列示目录（通常不推荐此做法）。
测试请求和响应：

```
GET /luci-static/resources/css/%2E/?version=5200 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1/cgi-bin/luci
Connection: Keep-Alive
Host: 192.168.1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Transfer-Encoding: chunked
Connection: Keep-Alive
Keep-Alive: timeout=20
Date: Tue, 01 Apr 2025 01:22:07 GMT
Content-Type: text/html

<html><head><title>Index of /luci-static/resources/css/</title></head><body><h1>Index of /luci-
static/resources/css/</h1><hr /><ol><li><strong><a href='/luci-static/resources/css/../'>..
</a>/</strong><br /><small>modified: Sat, 22 Jun 2024 08:13:57 GMT<br />directory - 0.17 kbyte<br
/><br /></small></li><li><strong><a href='/luci-
static/resources/css/appdownload.css'>appdownload.css</a></strong><br /><small>modified: Fri, 13
Nov 2020 07:23:58 GMT<br />text/css - 0.93 kbyte<br /><br /></small></li><li><strong><a
href='/luci-static/resources/css/backgroundsize.min.htc'>backgroundsize.min.htc</a></strong><br
/><small>modified: Fri, 13 Nov 2020 07:23:58 GMT<br />application/octet-stream - 5.76 kbyte<br />
<br /></small></li><li><strong><a href='/luci-static/resources/css/device.css'>device.css</a>
</strong><br /><small>modified: Fri, 13 Nov 2020 07:23:58 GMT<br />text/css - 1.75 kbyte<br /><br
/></small></li><li><strong><a href='/luci-static/resources/css/home_style.css'>home_style.css</a>
</strong><br /><small>modified: Fri, 15 Jul 2022 02:22:43 GMT<br />text/css - 11.65 kbyte<br />
<br /></small></li><li><strong><a href='/luci-static/resources/css/login.css'>login.css</a>
</strong><br /><small>modified: Fri, 13 Nov 2020 07:23:58 GMT<br />text/css - 5.37 kbyte<br /><br
/></small></li><li><strong><a href='/luci-static/resources/css/main_help.css'>main_help.css</a>
</strong><br /><small>modified: Fri, 13 Nov 2020 07:23:58 GMT<br />text/css - 3.42 kbyte<br /><br
/></small></li><li><strong><a href='/luci-
static/resources/css/main_portmap_list.css'>main_portmap_list.css</a></strong><br />
<small>modified: Fri, 13 Nov 2020 07:23:58 GMT<br />text/css - 0.84 kbyte<br /><br /></small>
</li><li><strong><a href='/luci-static/resources/css/main_style.css'>main_style.css</a></strong>
<br /><small>modified: Tue, 08 Aug 2023 01:48:18 GMT<br />text/css - 16.85 kbyte<br /><br />
</small></li><li><strong><a href='/luci-static/resources/css/register.css'>register.css</a>
</strong><br /><small>modified: Fri, 13 Nov 2020 07:23:58 GMT<br />text/css - 6.74 kbyte<br /><br
/></small></li><li><strong><a href='/luci-static/resources/css/storage.css'>storage.css</a>
</strong><br /><small>modified: Fri, 13 Nov 2020 07:23:58 GMT<br />text/css - 2.87 kbyte<br /><br
/></small></li><li><strong><a href='/luci-
static/resources/css/storage_settings.css'>storage_settings.css</a></strong><br />
<small>modified: Fri, 13 Nov 2020 07:23:58 GMT<br />text/css - 7.17 kbyte<br /><br /></small>
</li><li><strong><a href='/luci-static/resources/css/wifi.css'>wifi.css</a></strong><br />
<small>modified: Fri, 13 Nov 2020 07:23:58 GMT<br />text/css - 3.37 kbyte<br /><br /></small>
</li></ol><hr /></body></html>
```

测试响应



Index of /luci-static/resources/css/

1. ../
   modified: Sat, 22 Jun 2024 08:13:57 GMT
   directory - 0.17 kbyte
2. appdownload.css
   modified: Fri, 13 Nov 2020 07:23:58 GMT
   text/css - 0.93 kbyte
3. backgroundsize.min.htc
   modified: Fri, 13 Nov 2020 07:23:58 GMT
   application/octet-stream - 5.76 kbyte
4. device.css
   modified: Fri, 13 Nov 2020 07:23:58 GMT
   text/css - 1.75 kbyte
5. home_style.css
   modified: Fri, 15 Jul 2022 02:22:43 GMT
   text/css - 11.65 kbyte
6. login.css
   modified: Fri, 13 Nov 2020 07:23:58 GMT
   text/css - 5.37 kbyte
7. main_help.css
   modified: Fri, 13 Nov 2020 07:23:58 GMT
   text/css - 3.42 kbyte
8. main_portmap_list.css
   modified: Fri, 13 Nov 2020 07:23:58 GMT
   text/css - 0.84 kbyte
9. main_style.css
   modified: Tue, 08 Aug 2023 01:48:18 GMT
   text/css - 16.85 kbyte
10. register.css
    modified: Fri, 13 Nov 2020 07:23:58 GMT
    text/css - 6.74 kbyte
11. storage.css
    modified: Fri, 13 Nov 2020 07:23:58 GMT
    text/css - 2.87 kbyte
12. storage_settings.css
    modified: Fri, 13 Nov 2020 07:23:58 GMT
    text/css - 7.17 kbyte
13. wifi.css
    modified: Fri, 13 Nov 2020 07:23:58 GMT
    text/css - 3.37 kbyte

BEA WebLogic URL 欺骗目录列表

严重性：	中
CVSS 分数：	6.4
URL：	http://192.168.1.1/luci-static/resources/image/login/
实体：	login/ (Page)
风险：	可能会查看和下载特定 Web 应用程序虚拟目录的内容，其中可能包含受限文件
原因：	未安装第三方产品的最新补丁或最新修订程序
固定值：	安装 WebLogic 的最新版本和补丁

差异： **方法** 从以下位置进行控制： `HEAD` 至： `GET`
路径 从以下位置进行控制： `/luci-static/resources/image/login/login-tip.png` 至： `/luci-static/resources/image/login/%2E/`

推理： 响应包含目录的内容（目录列表）。这表示服务器允许列示目录（通常不推荐此做法）。
测试请求和响应：

```
GET /luci-static/resources/image/login/%2E/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1/cgi-bin/luci
Connection: Keep-Alive
Host: 192.168.1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Transfer-Encoding: chunked
Connection: Keep-Alive
Keep-Alive: timeout=20
Date: Tue, 01 Apr 2025 01:22:09 GMT
Content-Type: text/html

<html><head><title>Index of /luci-static/resources/image/login/</title></head><body><h1>Index of
/luci-static/resources/image/login/</h1><hr /><ol><li><strong><a href='/luci-
static/resources/image/login/../'>..</a>/</strong><br /><small>modified: Sat, 22 Jun 2024
08:13:57 GMT<br />directory - 0.88 kbyte<br /><br /></small></li><li><strong><a href='/luci-
static/resources/image/login/WIFI_name.png'>WIFI_name.png</a></strong><br /><small>modified: Fri,
13 Nov 2020 07:23:54 GMT<br />image/png - 0.80 kbyte<br /><br /></small></li><li><strong><a
href='/luci-static/resources/image/login/bg_round_b.png'>bg_round_b.png</a></strong><br />
<small>modified: Fri, 13 Nov 2020 07:23:54 GMT<br />image/png - 82.15 kbyte<br /><br /></small>
</li><li><strong><a href='/luci-static/resources/image/login/bg_round_s.png'>bg_round_s.png</a>
</strong><br /><small>modified: Fri, 13 Nov 2020 07:23:54 GMT<br />image/png - 71.85 kbyte<br />
<br /></small></li><li><strong><a href='/luci-
static/resources/image/login/bg_round_s_IE.png'>bg_round_s_IE.png</a></strong><br />
<small>modified: Fri, 13 Nov 2020 07:23:54 GMT<br />image/png - 73.15 kbyte<br /><br /></small>
</li><li><strong><a href='/luci-
static/resources/image/login/broadband_username.png'>broadband_username.png</a></strong><br />
<small>modified: Fri, 13 Nov 2020 07:23:54 GMT<br />image/png - 0.70 kbyte<br /><br /></small>
</li><li><strong><a href='/luci-static/resources/image/login/eye-open.png'>eye-open.png</a>
</strong><br /><small>modified: Fri, 13 Nov 2020 07:23:54 GMT<br />image/png - 0.62 kbyte<br />
<br /></small></li><li><strong><a href='/luci-
static/resources/image/login/eye_close.png'>eye_close.png</a></strong><br /><small>modified: Fri,
13 Nov 2020 07:23:54 GMT<br />image/png - 0.67 kbyte<br /><br /></small></li><li><strong><a
href='/luci-static/resources/image/login/login-tip.png'>login-tip.png</a></strong><br />
<small>modified: Fri, 13 Nov 2020 07:23:54 GMT<br />image/png - 14.28 kbyte<br /><br /></small>
</li><li><strong><a href='/luci-static/resources/image/login/login_password-
1.png'>login_password-1.png</a></strong><br /><small>modified: Fri, 13 Nov 2020 07:23:54 GMT<br
/>image/png - 0.47 kbyte<br /><br /></small></li><li><strong><a href='/luci-
static/resources/image/login/login_user-1.png'>login_user-1.png</a></strong><br />
<small>modified: Fri, 13 Nov 2020 07:23:54 GMT<br />image/png - 0.51 kbyte<br /><br /></small>
</li><li><strong><a href='/luci-
static/resources/image/login/register_loading_1.png'>register_loading_1.png</a></strong><br />
<small>modified: Fri, 13 Nov 2020 07:23:54 GMT<br />image/png - 0.52 kbyte<br /><br /></small>
</li><li><strong><a href='/luci-
```

```
static/resources/image/login/register_loading_2.png'>register_loading_2.png</a></strong><br />
<small>modified: Fri, 13 Nov 2020 07:23:54 GMT<br />image/png - 0.43 kbyte<br /><br /></small>
</li><li><strong><a href='/luci-static/resources/image/login/step1_tip.png'>step1_tip.png</a>
</strong><br /><small>modified: Fri, 13 Nov 2020 07:23:54 GMT<br />image/png - 41.67 kbyte<br />
<br /></small></li><li><strong><a href='/luci-
static/resources/image/login/step2_tip.png'>step2_tip.png</a></strong><br /><small>modified: Fri,
13 Nov 2020 07:23:54 GMT<br />image/png - 46.61 kbyte<br /><br /></small></li></ol><hr /></body>
</html>
```

问题 4 / 6

TOC

BEA WebLogic URL 欺骗目录列表

严重性：	中
CVSS 分数：	6.4
URL：	http://192.168.1.1/luci-static/resources/
实体：	resources/ (Page)
风险：	可能会查看和下载特定 Web 应用程序虚拟目录的内容，其中可能包含受限文件
原因：	未安装第三方产品的最新补丁或最新修订程序
固定值：	安装 WebLogic 的最新版本和补丁

差异： **路径** 从以下位置进行控制：`/luci-static/resources/js/util.js` 至：`/luci-static/resources/%2E/`

推理： 响应包含目录的内容（目录列表）。这表示服务器允许列示目录（通常不推荐此做法）。

测试请求和响应：

```
GET /luci-static/resources/%2E/?version=5200 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1/cgi-bin/luci
Connection: keep-alive
Host: 192.168.1.1
Accept: */*
Accept-Language: en-US


HTTP/1.1 200 OK
Transfer-Encoding: chunked
Connection: Keep-Alive
Keep-Alive: timeout=20
Date: Tue, 01 Apr 2025 01:21:56 GMT
Content-Type: text/html

<html><head><title>Index of /luci-static/resources/</title></head><body><h1>Index of /luci-
static/resources/</h1><hr /><ol><li><strong><a href='/luci-static/resources/../'>..</a>/</strong>
<br /><small>modified: Sat, 22 Jun 2024 08:13:57 GMT<br />directory - 0.05 kbyte<br /><br />
</small></li><li><strong><a href='/luci-static/resources/css/'>css</a>/</strong><br />
<small>modified: Sat, 22 Jun 2024 08:13:57 GMT<br />directory - 0.27 kbyte<br /><br /></small>
</li><li><strong><a href='/luci-static/resources/fonts/'>fonts</a>/</strong><br />
<small>modified: Sat, 22 Jun 2024 08:13:57 GMT<br />directory - 0.04 kbyte<br /><br /></small>
</li><li><strong><a href='/luci-static/resources/image/'>image</a>/</strong><br />
<small>modified: Sat, 22 Jun 2024 08:13:57 GMT<br />directory - 0.88 kbyte<br /><br /></small>
</li><li><strong><a href='/luci-static/resources/js/'>js</a>/</strong><br /><small>modified: Sat,
22 Jun 2024 08:13:57 GMT<br />directory - 0.27 kbyte<br /><br /></small></li><li><strong><a
href='/luci-static/resources/bandwidth.svg'>bandwidth.svg</a></strong><br /><small>modified: Fri,
13 Nov 2020 07:23:49 GMT<br />image/svg+xml - 0.89 kbyte<br /><br /></small></li><li><strong><a
href='/luci-static/resources/connections.svg'>connections.svg</a></strong><br /><small>modified:
Fri, 13 Nov 2020 07:23:49 GMT<br />image/svg+xml - 0.99 kbyte<br /><br /></small></li><li>
```

```
<strong><a href='/luci-static/resources/load.svg'>load.svg</a></strong><br /><small>modified:
Fri, 13 Nov 2020 07:23:49 GMT<br />image/svg+xml - 1.01 kbyte<br /><br /></small></li><li>
<strong><a href='/luci-static/resources/wifirate.svg'>wifirate.svg</a></strong><br />
<small>modified: Fri, 13 Nov 2020 07:23:49 GMT<br />image/svg+xml - 0.80 kbyte<br /><br />
</small></li><li><strong><a href='/luci-static/resources/wireless.svg'>wireless.svg</a></strong>
<br /><small>modified: Fri, 13 Nov 2020 07:23:49 GMT<br />image/svg+xml - 0.89 kbyte<br /><br />
</small></li><li><strong><a href='/luci-static/resources/xhr.js'>xhr.js</a></strong><br />
<small>modified: Thu, 25 Jan 2024 01:51:35 GMT<br />text/javascript - 4.84 kbyte<br /><br />
</small></li></ol><hr /></body></html>
```

问题 5 / 6

TOC

BEA WebLogic URL 欺骗目录列表

严重性：	中
CVSS 分数：	6.4
URL：	http://192.168.1.1/luci-static/resources/js/
实体：	js/ (Page)
风险：	可能会查看和下载特定 Web 应用程序虚拟目录的内容，其中可能包含受限文件
原因：	未安装第三方产品的最新补丁或最新修订程序
固定值：	安装 WebLogic 的最新版本和补丁

差异： **路径** 从以下位置进行控制：`/luci-static/resources/js/util.js` 至：`/luci-static/resources/js/%2E/`

推理： 响应包含目录的内容（目录列表）。这表示服务器允许列示目录（通常不推荐此做法）。

测试请求和响应：

```
GET /luci-static/resources/js/%2E/?version=5200 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1/cgi-bin/luci
Connection: keep-alive
Host: 192.168.1.1
Accept: */*
Accept-Language: en-US


HTTP/1.1 200 OK
Transfer-Encoding: chunked
Connection: Keep-Alive
Keep-Alive: timeout=20
Date: Tue, 01 Apr 2025 01:21:57 GMT
Content-Type: text/html

<html><head><title>Index of /luci-static/resources/js/</title></head><body><h1>Index of /luci-
static/resources/js/</h1><hr /><ol><li><strong><a href='/luci-static/resources/js/../'>..
</a>/</strong><br /><small>modified: Sat, 22 Jun 2024 08:13:57 GMT<br />directory - 0.17 kbyte<br
/><br /></small></li><li><strong><a href='/luci-static/resources/js/device.js'>device.js</a>
</strong><br /><small>modified: Mon, 15 Mar 2021 07:40:43 GMT<br />text/javascript - 5.95
kbyte<br /><br /></small></li><li><strong><a href='/luci-
static/resources/js/highcharts.js'>highcharts.js</a></strong><br /><small>modified: Fri, 13 Nov
2020 07:23:59 GMT<br />text/javascript - 149.70 kbyte<br /><br /></small></li><li><strong><a
href='/luci-static/resources/js/jquery.js'>jquery.js</a></strong><br /><small>modified: Fri, 13
Nov 2020 07:23:59 GMT<br />text/javascript - 84.89 kbyte<br /><br /></small></li><li><strong><a
href='/luci-static/resources/js/jquery.nicescroll.min.js'>jquery.nicescroll.min.js</a></strong>
<br /><small>modified: Fri, 13 Nov 2020 07:23:59 GMT<br />text/javascript - 60.92 kbyte<br /><br
/></small></li><li><strong><a href='/luci-static/resources/js/login.js'>login.js</a></strong><br
/><small>modified: Tue, 05 Mar 2024 01:09:21 GMT<br />text/javascript - 4.06 kbyte<br /><br />
```

```
</small></li><li><strong><a href='/luci-static/resources/js/main.js'>main.js</a></strong><br />
<small>modified: Thu, 09 Nov 2023 08:48:30 GMT<br />text/javascript - 16.37 kbyte<br /><br />
</small></li><li><strong><a href='/luci-static/resources/js/main_home.js'>main_home.js</a>
</strong><br /><small>modified: Mon, 15 Mar 2021 07:40:43 GMT<br />text/javascript - 12.37
kbyte<br /><br /></small></li><li><strong><a href='/luci-
static/resources/js/main_portmap_list.js'>main_portmap_list.js</a></strong><br /><small>modified:
Fri, 13 Nov 2020 07:23:59 GMT<br />text/javascript - 2.13 kbyte<br /><br /></small></li><li>
<strong><a href='/luci-static/resources/js/mesh.js'>mesh.js</a></strong><br /><small>modified:
Thu, 21 Jan 2021 02:51:35 GMT<br />text/javascript - 4.54 kbyte<br /><br /></small></li><li>
<strong><a href='/luci-static/resources/js/register.js'>register.js</a></strong><br />
<small>modified: Wed, 03 Apr 2024 10:01:23 GMT<br />text/javascript - 20.01 kbyte<br /><br />
</small></li><li><strong><a href='/luci-static/resources/js/util.js'>util.js</a></strong><br />
<small>modified: Tue, 05 Mar 2024 01:09:21 GMT<br />text/javascript - 40.65 kbyte<br /><br />
</small></li><li><strong><a href='/luci-
static/resources/js/wifi_advanced.js'>wifi_advanced.js</a></strong><br /><small>modified: Fri, 13
Nov 2020 07:23:59 GMT<br />text/javascript - 1.28 kbyte<br /><br /></small></li><li><strong><a
href='/luci-static/resources/js/wifi_basic.js'>wifi_basic.js</a></strong><br /><small>modified:
Fri, 13 Nov 2020 07:23:59 GMT<br />text/javascript - 2.16 kbyte<br /><br /></small></li></ol><hr
/></body></html>
```


问题 6 / 6

TOC

BEA WebLogic URL 欺骗目录列表

严重性：	中
CVSS 分数：	6.4
URL：	http://192.168.1.1/luci-static/
实体：	luci-static/ (Page)
风险：	可能会查看和下载特定 Web 应用程序虚拟目录的内容，其中可能包含受限文件
原因：	未安装第三方产品的最新补丁或最新修订程序
固定值：	安装 WebLogic 的最新版本和补丁

差异： **路径** 从以下位置进行控制：`/luci-static/resources/js/util.js` 至：`/luci-static/%2E/`

推理： 响应包含目录的内容（目录列表）。这表示服务器允许列示目录（通常不推荐此做法）。

测试请求和响应：


```
GET /luci-static/%2E/?version=5200 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1/cgi-bin/luci
Connection: keep-alive
Host: 192.168.1.1
Accept: */*
Accept-Language: en-US


HTTP/1.1 200 OK
Transfer-Encoding: chunked
Connection: Keep-Alive
Keep-Alive: timeout=20
Date: Tue, 01 Apr 2025 01:21:57 GMT
Content-Type: text/html

<html><head><title>Index of /luci-static/</title></head><body><h1>Index of /luci-static/</h1><hr
/><ol><li><strong><a href='/luci-static/../'>..</a>/</strong><br /><small>modified: Fri, 01 Sep
2023 10:40:43 GMT<br />directory - 0.07 kbyte<br /><br /></small></li><li><strong><a href='/luci-
static/bootstrap/'>bootstrap</a>/</strong><br /><small>modified: Sat, 22 Jun 2024 08:13:57 GMT<br
/>directory - 0.08 kbyte<br /><br /></small></li><li><strong><a href='/luci-
```

```
static/resources/'>resources</a>/</strong><br /><small>modified: Sat, 22 Jun 2024 08:13:57 GMT<br
/>directory - 0.17 kbyte<br /><br /></small></li></ol><hr /></body></html>
```

低 “Content-Security-Policy”头缺失或不安全 5 TOC

问题 1 / 5 TOC

“Content-Security-Policy”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1/
实体：	(Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用安全策略的“Content-Security-Policy”头

差异：

推理： AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

测试请求和响应：

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: 192.168.1.1
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Last-Modified: Thu, 10 Nov 2022 02:15:45 GMT
Connection: Keep-Alive
Content-Length: 444
X-Frame-Options: SAMEORIGIN
Keep-Alive: timeout=20
ETag: "15a-1bc-636c5ed1"
Date: Tue, 01 Apr 2025 01:20:47 GMT
Content-Type: text/html

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=Edge">
<meta http-equiv="refresh" content="0; URL=/cgi-bin/luci" />
<meta HTTP-EQUIV="pragma" CONTENT="no-cache">
<meta HTTP-EQUIV="Cache-Control" CONTENT="no-store, must-revalidate">
<meta HTTP-EQUIV="expires" CONTENT="0">
<title>中国电信智能网关</title>
```

```
</head>
<body>
</body>
</html>


GET /cgi-bin/luci HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1/
Connection: Keep-Alive
Host: 192.168.1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Transfer-Encoding: chunked
Connection: Keep-Alive
X-Frame-Options: SAMEORIGIN
X-Frame-Options: SAMEORIGIN
Keep-Alive: timeout=20
Cache-Control: no-cache
Expires: 0
Content-Type: text/html; charset=utf-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>
  <head>
  <meta http-equiv='Content-Type' content='text/html; charset=utf-8'/>
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
 <meta HTTP-EQUIV="pragma" CONTENT="no-cache">
 <meta HTTP-EQUIV="Cache-Control" CONTENT="no-store, must-revalidate">
 <meta HTTP-EQUIV="expires" CONTENT="0">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <title>中国电信智能网关</title>
  <link rel="shortcut icon" href="/luci-static/resources/image/favicon.ico">
  <link rel="bookmark" href="/luci-static/resources/image/favicon.ico">
  <link href="/luci-static/resources/css/login.css?version=5200" rel="stylesheet">
  <script src="/luci-static/resources/js/jquery.js?version=5200"></script>
  <script src="/luci-static/resources/js/util.js?version=5200"></script>
  <script src="/luci-static/resources/js/login.js?version=5200"></script>
  <script>

 window.onload =function() {console.log("The device support WiFi: " + 1);

 console.log("The device support USB: " + 1);

 console.log("The device type: " + 9);

 window.localStorage.setItem("hasWiFi", 1);
 window.localStorage.setItem("hasPots", 1);
 window.localStorage.setItem("hasUsb", 1);
 window.localStorage.setItem("hasMesh", 1);
 window.localStorage.setItem("devType", 9);
        }

        function hideHint()
        {
                $(".login-input").children(":last").remove();
                $("#login_username").removeAttr("disabled");
         $("#login_password").removeAttr("disabled");
        }
  </script>
  </head>
  <body onkeydown='keyCapscheck(event, 1)'>
  <div class="login_bg">
 <form method="post" id="argform">
         <input type="hidden" name="username" id="username" value="telecomadmin" />
         <input type="hidden" name="psd" id="psd" value="" />
         <input type="submit" style="display:none"/>
 </form><div class="logo"><img src="/luci-static/resources/image/logo_tianyi.png"
alt="logo"></div>
    <div class="line" id="line" name="line">
      <table align=left cellpadding=0 cellspace=0 border=0>
        <tr>
          <td id="line1" name="line1" valign="top">
```

```
          <img src="/luci-static/resources/image/line.png" style="opacity:0.2;">
        </td>
        <td id="line2" name="line2" valign="top">
          <img src="/luci-static/resources/image/line.png" style="margin-left:-3px;opacity:0.2;">
        </td>
        </tr>
      </table>
    </div>
    <script>
    if (bType == "IE8")
    {
         var speed=6;
         console.log("Current broswer is IE8.");
     function Marquee(){
       if(document.getElementById("line2").offsetWidth-
document.getElementById("line").scrollLeft<=0)
         document.getElementById("line").scrollLeft-
=document.getElementById("line1").offsetWidth;
       else{
         document.getElementById("line").scrollLeft++;
       }
     }
         setInterval(Marquee,speed);
        }
    </script>
    <div id='copyright_div'>
   Copyright (C) 2015        中国电信 All rights reserved.  
   <script>
         function isIPv6Addr(str)
                {
                 return /:/.test(str) &&
                   str.match(/:/g).length<8 &&
                   /::/.test(str)
                   ?(str.match(/::/g).length==1 &&
                   /^::$|^(::)?([\da-f]{1,4}(:|::))*[\da-f]{1,4}(:|::)?$/i.test(str))
                   :/^([\da-f]{1,4}:){7}[\da-f]{1,4}$/i.test(str);
                }

         if (isIPv6Addr(location.host))
                 var hosturl = "[" + location.
...
...
...
```

问题 2 / 5

TOC

“Content-Security-Policy”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1:8080/maintain
实体：	maintain (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用安全策略的“Content-Security-Policy”头

差异：

推理： AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴

露于各种跨站点注入攻击之下

测试请求和响应：

```
GET /maintain HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1/cgi-bin/luci
Connection: keep-alive
Host: 192.168.1.1:8080
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 1582
Content-Type:

<!DOCTYPE html>
<html lang="en">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge">
 <meta name="viewport" content="width=device-width, initial-scale=1">
 <meta HTTP-EQUIV='Pragma' CONTENT='no-cache'>
 <title>       中国电信智能网关</title>
 <link href="/css/login.css?v=20250327153146" rel="stylesheet">
 <link href="/css/main_style.css?v=20250327153146" rel="stylesheet">
 <script src="/js/jquery.js?v=20250327153146"></script>
 <script src="/js/aes_1.js?v=20250327153146"></script>
 <script src="/js/common.js?v=20250327153146"></script>
  <script>
         var g_wlan24_num=8
         var g_wlan58_num=8
         var g_usb_num=1
         var g_province="JT"
  </script>
</head>
<body>
 <script>
     if (g_province == "JT" || g_province == "HAI") {
         window.location="/";
     } else {
         window.location="/register.html";
     }
 </script>       <div id="pop_window_div" style="display: none;"></div>
 <div id="pop_window_content_div" style="display: none;">
         <div id="pop_window_title"></div>
         <div id="pop_window_body">
                 <div id="pop_window_icon"></div>
                 <div id="pop_window_show_div">
                         <div id="pop_window_loading"></div>
                         <div id="pop_window_message"></div>
                         <div id="pop_window_option">
                                 <div id="pop_window_confirm" class="pop_window_action
bg_color_main">确认</div>
                                 <div id="pop_window_cancel" class="pop_window_action
bg_color_red">取消</div>
                         </div>
                 </div>
         </div>
 </div>
 <div id="loading" style="display: none;">
         <div id="loading_content">
                 <img src="/image/loading.gif">
         </div>
 </div>
</body>
</html>
```

“Content-Security-Policy”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1/luci-static/resources/js/util.js
实体：	util.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用安全策略的“Content-Security-Policy”头

差异：

推理： AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

测试请求和响应：

```
GET /luci-static/resources/js/util.js?version=5200 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1/cgi-bin/luci
Connection: keep-alive
Host: 192.168.1.1
Accept: */*
Accept-Language: en-US


HTTP/1.1 200 OK
Last-Modified: Tue, 05 Mar 2024 01:09:21 GMT
Connection: Keep-Alive
Content-Length: 41626
Keep-Alive: timeout=20
ETag: "d6-a29a-65e670c1"
Date: Tue, 01 Apr 2025 01:20:48 GMT
Content-Type: text/javascript

var WEB_POLL_INTERVAL=5;

window.console = window.console || (function(){
    var c = {}; c.log = c.warn = c.debug = c.info = c.error = c.time = c.dir = c.profile
    = c.clear = c.exception = c.trace = c.assert = function(){};
    return c;
})();

var noWiFi = (window.localStorage.getItem("hasWiFi") == 1) ? 0 : 1;
var noPots = (window.localStorage.getItem("hasPots") == 1) ? 0 : 1;
var noUsb = (window.localStorage.getItem("hasUsb") == 1) ? 0 : 1;
var noMesh = (window.localStorage.getItem("hasMesh") == 1) ? 0 : 1;
var devType = window.localStorage.getItem("devType");

function isIE7Browser()
{
 if(navigator.appName == "Microsoft Internet Explorer" &&
navigator.appVersion.match(/7./i)=="7.")
 {
         return true;
        }
 else
        {
         return false;
        }
}
function judedNavation()
```

```
{
 if(navigator.appName == "Microsoft Internet Explorer" &&
navigator.appVersion.match(/6./i)=="6."){
         return 6;
 }
 else if(navigator.appName == "Microsoft Internet Explorer" &&
navigator.appVersion.match(/7./i)=="7."){
         return 7;
 }
 else if(navigator.appName == "Microsoft Internet Explorer" &&
navigator.appVersion.match(/8./i)=="8."){
         return 8;
 }
 else if(navigator.appName == "Microsoft Internet Explorer" &&
navigator.appVersion.match(/9./i)=="9."){
         return 9;
        }
 else{
         return 10;
        }
}


function createInput(id, name, placeholder, maxlength, type, value)
{
 var inputObj = "<input ";
 if ( id != "" && id != "undefined" )
        {
         inputObj += "id='" + id + "' ";
        }
 if ( name != "" && name != "undefined" )
        {
         inputObj += "name='" + name + "' ";
        }
 if ( placeholder != "" && placeholder != "undefined" )
        {
         inputObj += "placeholder='" + placeholder + "' ";
        }
 if ( maxlength != "" && maxlength != "undefined" )
        {
         inputObj += "maxlength='" + maxlength + "' ";
        }
 inputObj += "type='" + type + "' ";
 inputObj += "value='" + value + "' ";
 inputObj += ">";
 return inputObj;
}

function inputBindFocus()
{
 $("input[type='password'], .password_content input[type='text']").bind("focusin",
function(){
         $(this).parent().eq(0).addClass("password_content_focus");
         if ( !$(this).next().hasClass("password_switch_eyeon") )
                {
         $(this).next().addClass("password_switch_focus");
                }
 });
 $("input[type='password'], .password_content input[type='text']").bind("focusout",
function(){
         $(this).parent().eq(0).removeClass("password_content_focus");
         $(this).next().removeClass("password_switch_focus");
 });
}

function customSwitchInit()
{
 $(".switch_content").bind("click", function(){
         if($(this).hasClass("switch_content_on")){
                 $(this).removeClass("switch_content_on");
                 $(this).addClass("switch_content_off");
                 $(this).children("span").html("OFF ");
                 $("#" + $(this).attr("id") + "_value").val(0);
         }else{
                 $(this).addClass("switch_content_on");
                 $(this).removeClass("switch_content_off");
                 $(this).children("span").html(" ON");
                 $("#" + $(this).attr("id") + "_value").val(1);
```

```
                }
         console.log($("#" + $(this).attr("id") + "_value").val());
 });
}
function customSelectInit()
{
 $(".select-arrow").click(function(){
         $(this).parent().addClass("select-open");
        });

 //Èç¹ûÊó±êÏòÏÂ»¬¶¯£¬Ôò²»Òþ²Ø
 $(".dropdown-select").bind("mouseleave",
                 function(e)
                 {
                         var w = $(this).width();
                         var h = $(this).height();
                         var x = (e.pageX - this.offsetLeft - (w / 2)) * (w > h ? (h / w)
: 1);
                         var y = (e.pageY - this.offsetTop - (h / 2)) * (h > w ? (w / h) :
1);
                         var direction = Math.round((((Math.atan2(y, x) * (180 / Math.PI))
+ 180) / 90) + 3) % 4;
                         if(direction != 2)
                         {
                                 $(this).removeClass("select-open");
                                }
 });

 $(".dropdown-menu-select").mouseleave(function(){
        $(this).parent().removeClass("select-open");
 });

 $(".dropdown-menu-select li").click(function(){
         $(this).parent().siblings("label").first().text($(this).text());
         $("#" + $(this).parent().attr("id") + "_value").val($(this).attr("livalue"));
         $(this).parent().parent().removeClass("select-open");;
 });
}
function customPasswordInit()
{
 inputBindFocus();
 $(".password_switch").bind("click", function(){
         if( $(this).css("background-image").indexOf("eye_close") > -1 )
                {
                 $(this).removeClass("password_switch_unfocus");
                 $(this).removeClass("password_switch_focus");
                 $(this).addClass("password_switch_eyeon");
                }
         else
                {
                 $(this).removeClass("password_switch_eyeon");
                 $(this).addClass("password_switch_unfocus");
                }

         if( 9 > judedNavation() )
                {
                 var $pwdInput =
...
...
...
```

“Content-Security-Policy”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1:8080/js/aes_1.js
实体：	aes_1.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用安全策略的“Content-Security-Policy”头

差异：

推理： AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

测试请求和响应：

```
GET /js/aes_1.js?v=20250327153146 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1:8080/maintain
Connection: keep-alive
Host: 192.168.1.1:8080
Accept: */*
Accept-Language: en-US


HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 19061
Cache-control: public,max-age=86400
Content-Type: application/x-javascript

var passwd_key = ""
function encryted_pwd(pwd){
 var key = "";
 for(var i = 0; i < passwd_key.length; i++){
         if(passwd_key.charCodeAt(i) < 16){
                 key += ("0" + (passwd_key.charCodeAt(i)).toString(16));
                }
         else{
                 key += (passwd_key.charCodeAt(i)).toString(16);
                }
        }
 if (key.length > 64){
         key = key.slice(0,64);
        }
 else{
         for (var i = key.length; i < 64 ; i++){
                 key += "0";
                }
        }
 key = CryptoJS.enc.Hex.parse(key);
 return en_func(pwd,key);
}

var Crypto_aes_g_key = "6873616E000000000000000000000000000000000000000000000000000000000000000000000000";

function encrypt_info(pwd){
 var key = CryptoJS.enc.Hex.parse(Crypto_aes_g_key);
 return en_func(pwd,key);
}

function en_func(pwd,key){
 var ivRand = randNum(16);
 pwd = CryptoJS.enc.Utf8.parse(pwd);
```

```
 var encryptedPwd = CryptoJS.AES.encrypt(pwd, key, {
     //iv: CryptoJS.enc.Utf8.parse("0000000000000000"),
     iv: CryptoJS.enc.Hex.parse(ivRand),
     mode: CryptoJS.mode.CBC,
     padding: CryptoJS.pad.Pkcs7
 });

 var encryptedPwdStr = encryptedPwd.ciphertext.toString();
 //return encryptedBase64Str;
 var ivEncryptedPwd = ivRand + encryptedPwdStr;
 return ivEncryptedPwd;
}

function randNum(n){
    var rnd = "";
    var rndIv = "";
    for(var i=0;i<n;i++){
        rnd = Math.floor(Math.random()*256);
        if(rnd<16)
                rnd = "0" + rnd.toString(16);
         else
                rnd = rnd.toString(16);
         rndIv += rnd;
    }
    return rndIv;
}

function decrypt_info(encryptedIvPwd){
 var key = CryptoJS.enc.Hex.parse(Crypto_aes_g_key);
 var ivRecived = encryptedIvPwd.slice(0,32);
 var encryptedPwd = encryptedIvPwd.slice(32,encryptedIvPwd.length);
 var encryptedHexStr = CryptoJS.enc.Hex.parse(encryptedPwd);
    var encryptedBase64Str = CryptoJS.enc.Base64.stringify(encryptedHexStr);

    var decryptedData = CryptoJS.AES.decrypt(encryptedBase64Str, key, {
     //iv: CryptoJS.enc.Utf8.parse("0000000000000000"),
     iv: CryptoJS.enc.Hex.parse(ivRecived),
     mode: CryptoJS.mode.CBC,
     padding: CryptoJS.pad.Pkcs7
 });

    var decryptedStr = decryptedData.toString(CryptoJS.enc.Utf8);
    return decryptedStr.toString();
}

var hexMap = new Array('0', '1', '2', '3', '4', '5', '6', '7', '8', '9', 'A', 'B', 'C', 'D', 'E',
'F');

function getDHprvkey(){
 var dhPrvKey = "";
 dhPrvKey += (Math.floor(Math.random() * 15)).toString(16);
 for (var j = 0; j < 191; j++){
         dhPrvKey += (Math.floor(Math.random() * 16)).toString(16);
        }

 return dhPrvKey;
}

function getDHkey(g,n,p){
 var g_Bigint = Bigint.fromHex(g);
 var n_Bigint = Bigint.fromHex(n);
 var p_Bigint = Bigint.fromHex(p);
 var dhKey = Bigint._powmod(g_Bigint,n_Bigint,p_Bigint);
 var dhKey_binary = dhKey.toBinaryString();
 var dhKey_tmp = "";
 var tmp,tmpLen;
 for (var i=dhKey_binary.length-1; i >= 0; i=i-4){
         if ((i-3)<0){
                 tmp = dhKey_binary.slice(0,i+1);
                 tmpLen = 4 - tmp.length;
                 for (var j = 0; j < tmpLen; j++) {
                         tmp = "0" + tmp;
                        }
                }
         else
                 tmp = dhKey_binary.slice(i-3,i+1);
         dhKey_tmp = hexMap[((tmp[0]=='1')?8:0)+((tmp[1]=='1')?4:0)+((tmp[2]=='1')?2:0)+
((tmp[3]=='1')?1:0)] + dhKey_tmp;
```

```
        }
 if(dhKey_tmp.length % 2 == 1)
         dhKey_tmp = "0" + dhKey_tmp;
 return dhKey_tmp;
}

function genDHkey(data,privkey,p){
    data = eval("("+data+")");
 if(data.data.web_stuff){
          var keysuff = '', exclus = '', aeskey = '';
          keysuff = getDHkey(data.data.web_stuff, privkey, p);
          var hex1 = 0, hex2 = 0, hex3 = 0, dec = 0, len = keysuff.length/3;
          for(var i = 0; i < len; i+=2){
          hex1 = '0x'+keysuff.slice(i, i+2);
          hex2 = '0x'+keysuff.slice(i+len, i+len+2);
          hex3 = '0x'+keysuff.slice(i+2*len, i+2*len+2);
         dec = hex1 ^ hex2 ^ hex3;
         exclus = dec.toString(16);
         if(exclus.length < 2){
                         exclus = "0" + exclus;
                }
         aeskey += exclus;
     }
     Crypto_aes_g_key = aeskey;
        }
    else{
        Crypto_aes_g_key = "6873616E0000000000000000000000000000000000000000000000000000000000000000";
    }
}

var CryptoJS=CryptoJS||function(u,p){
 var d={},l=d.lib={},s=function(){},t=l.Base={extend:function(a){
                 s.prototype=this;
                 var c=new s;
                 a&&c.mixIn(a);
                 c.hasOwnProperty("init")||(c.init=function(){
                         c.$super.init.apply(this,arguments);
                 })       ;
                 c.init.prototype=c;
                 c.$super=this;
                 return c;
         }       ,
         create:function(){
                 var a=this.extend();
                 a.init.apply(a,arguments);
                 return a;
         }       ,
         init:function(){},
         mixIn:function(a){
                 for(var c in a)
                         a.hasOwnProperty(c)&&(this[c]=a[c]);
                 a.hasOwnProperty("toString")&&(this.toString=a.toString);
         }       ,
         clone:fun
...
...
...
```

问题 5 / 5

TOC

“Content-Security-Policy”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1:8080/js/common.js
实体：	common.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用安全策略的“Content-Security-Policy”头

差异：

推理： AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

测试请求和响应：

```
GET /js/common.js?v=20250327153146 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1:8080/maintain
Connection: keep-alive
Host: 192.168.1.1:8080
Accept: */*
Accept-Language: en-US


HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 22938
Cache-control: public,max-age=86400
Content-Type: application/x-javascript

function web_server_result(s) {
 if (s == "null error") {
         return "        某些项的值无效，请重新填写"
 } else if (s == "data error") {
         return "        某些项的值无效，请重新填写"
 } else if (s == "set error") {
         return "        设置失败"
 } else if (s == "add error") {
         return "        添加失败"
 } else if (s == "del error") {
         return "        删除失败"
 } else if (s == "get error") {
         return "        获取配置失败"
 } else {
         return s
        }
}

function common_ajax_success(rsp, status, xhr) {
 var rsp_obj = rsp
 if (typeof(rsp) == "string")
         rsp_obj = JSON.parse(rsp)

 if (typeof(rsp_obj) == "object" && rsp_obj.retcode == "0" && rsp_obj.data.result ==
"SUCCESS") {
         location.reload()
 } else {
         var msg = ""
         if (rsp_obj.data && rsp_obj.data.errinfo) {
                 msg = msg + web_server_result(rsp_obj.data.errinfo)
                }
         if (rsp_obj.data && rsp_obj.data.result) {
                 msg = msg + rsp_obj.data.result
```

```
                }
         if (msg == "") {
                 msg = "       未知的错误"
                }

         pop_window.alert({title:"       警告", text:msg, confirm:true})
        }
}

function common_ajax_success_cb(rsp, status, xhr, cb) {
 var rsp_obj = rsp
 if (typeof(rsp) == "string")
         rsp_obj = JSON.parse(rsp)

 if (typeof(rsp_obj) == "object" && rsp_obj.retcode == "0" && rsp_obj.data.result ==
"SUCCESS") {
         cb()
 } else {
         var msg = ""
         if (rsp_obj.data && rsp_obj.data.errinfo) {
                 msg = msg + web_server_result(rsp_obj.data.errinfo)
                }
         if (rsp_obj.data && rsp_obj.data.result) {
                 msg = msg + rsp_obj.data.result
                }
         if (msg == "") {
                 msg = "       未知的错误"
                }

         pop_window.alert({title:"       警告", text:msg, confirm:true})
        }
}

function getQueryVariable(variable) {
    let query = window.location.search.substring(1);
    let vars = query.split("&");
    for (let i = 0; i < vars.length; i++) {
        let pair = vars[i].split("=");
        if (pair[0] == variable) {
          return pair[1];
        }
    }
}

function hasClass (ele, className) {
 var reg = new RegExp('(^|\\s)' + className + '(\\s|$)')
 return reg.test(ele.className)
}

function macToNumber(mac) {
 return Number("0x"+mac.replaceAll(':',''))
}

function ipToNumber(ip) {
 var num = 0;
 if(ip == "") {
         return num;
 }
    var aNum = ip.split(".");
    if(aNum.length != 4) {
        return num;
    }
    num += parseInt(aNum[0]) << 24;
    num += parseInt(aNum[1]) << 16;
    num += parseInt(aNum[2]) << 8;
    num += parseInt(aNum[3]) << 0;
    num = num >>> 0;//这个很关键，不然可能会出现负数的情况
    return num;
}

function numberToIp(number) {
    var ip = "";
    if(number <= 0) {
        return ip;
    }
    var ip3 = (number << 0 ) >>> 24;
    var ip2 = (number << 8 ) >>> 24;
    var ip1 = (number << 16) >>> 24;
```

```
    var ip0 = (number << 24) >>> 24

    ip += ip3 + "." + ip2 + "." + ip1 + "." + ip0;

    return ip;
}

function ipv4_prefix(ip) {
 var arr = ip.split('.')
 delete arr[3]
 return arr.join('.')
}

function is_ipv4(ip) {
 return /^(1\d{2}|2[0-4]\d|25[0-5]|[1-9]\d|[0-9])\.((1\d{2}|2[0-4]\d|25[0-5]|[1-
9]\d|\d)\.){2}(1\d{2}|2[0-4]\d|25[0-5]|[1-9]\d|\d)$/.test(ip)
}

function is_ipv6(ip) {
 return /^([\da-fA-F]{1,4}:){6}((25[0-5]|2[0-4]\d|[01]?\d\d?)\.){3}(25[0-5]|2[0-4]\d|[01]?
\d\d?)$|^::([\da-fA-F]{1,4}:){0,4}((25[0-5]|2[0-4]\d|[01]?\d\d?)\.){3}(25[0-5]|2[0-4]\d|[01]?
\d\d?)$|^([\da-fA-F]{1,4}::([\da-fA-F]{1,4}:){0,3}((25[0-5]|2[0-4]\d|[01]?\d\d?)\.){3}(25[0-
5]|2[0-4]\d|[01]?\d\d?)$|^([\da-fA-F]{1,4}:){2}:([\da-fA-F]{1,4}:){0,2}((25[0-5]|2[0-4]\d|[01]?
\d\d?)\.){3}(25[0-5]|2[0-4]\d|[01]?\d\d?)$|^([\da-fA-F]{1,4}:){3}:([\da-fA-F]{1,4}:){0,1}((25[0-
5]|2[0-4]\d|[01]?\d\d?)\.){3}(25[0-5]|2[0-4]\d|[01]?\d\d?)$|^([\da-fA-F]{1,4}:){4}:((25[0-5]|2[0-
4]\d|[01]?\d\d?)\.){3}(25[0-5]|2[0-4]\d|[01]?\d\d?)$|^([\da-fA-F]{1,4}:){7}[\da-fA-F]{1,4}$|^:((:
[\da-fA-F]{1,4}){1,6}|:)$|^[\da-fA-F]{1,4}:((:[\da-fA-F]{1,4}){1,5}|:)$|^([\da-fA-F]{1,4}:){2}((:
[\da-fA-F]{1,4}){1,4}|:)$|^([\da-fA-F]{1,4}:){3}((:[\da-fA-F]{1,4}){1,3}|:)$|^([\da-fA-F]{1,4}:)
{4}((:[\da-fA-F]{1,4}){1,2}|:)$|^([\da-fA-F]{1,4}:){5}:([\da-fA-F]{1,4})?$|^([\da-fA-F]{1,4}:)
{6}:$/.test(ip)
}

function is_domain(domain) {
 return /^(?=^.{3,255}$)[a-zA-Z0-9][-a-zA-Z0-9]{0,62}(\.[a-zA-Z0-9][-a-zA-Z0-9]
{0,62})+$/.test(domain)
}

function is_hex(s) {
 for (var i in s) {
         if (!((s[i].charCodeAt() >= '0'.charCodeAt() && s[i].charCodeAt() <=
'9'.charCodeAt()) ||
                 (s[i].charCodeAt() >= 'a'.charCodeAt() && s[i].charCodeAt() <=
'f'.charCodeAt()) ||
                 (s[i].charCodeAt() >= 'A'.charCodeAt() && s[i].charCodeAt() <=
'F'.charCodeAt())))
                {
                 return false
                }
        }

 return true
}

function iform_data() {
    var data = {}
    $.each($("iform select:enabled"), function(i, select){
        data[select.name] = s
...
...
...
```

低 “X-Content-Type-Options”头缺失或不安全 5 TOC

问题 1 / 5 TOC

“X-Content-Type-Options”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1/
实体：	(Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

差异：

推理： AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值，这可能会更大程度地暴露于偷渡式下载攻击之下

测试请求和响应：

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: 192.168.1.1
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Last-Modified: Thu, 10 Nov 2022 02:15:45 GMT
Connection: Keep-Alive
Content-Length: 444
X-Frame-Options: SAMEORIGIN
Keep-Alive: timeout=20
ETag: "15a-1bc-636c5ed1"
Date: Tue, 01 Apr 2025 01:20:47 GMT
Content-Type: text/html

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=Edge">
<meta http-equiv="refresh" content="0; URL=/cgi-bin/luci" />
<meta HTTP-EQUIV="pragma" CONTENT="no-cache">
<meta HTTP-EQUIV="Cache-Control" CONTENT="no-store, must-revalidate">
<meta HTTP-EQUIV="expires" CONTENT="0">
<title>中国电信智能网关</title>

</head>
<body>
</body>
</html>


GET /cgi-bin/luci HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1/
Connection: Keep-Alive
Host: 192.168.1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Transfer-Encoding: chunked
Connection: Keep-Alive
```

```
X-Frame-Options: SAMEORIGIN
X-Frame-Options: SAMEORIGIN
Keep-Alive: timeout=20
Cache-Control: no-cache
Expires: 0
Content-Type: text/html; charset=utf-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>
  <head>
  <meta http-equiv='Content-Type' content='text/html; charset=utf-8'/>
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
 <meta HTTP-EQUIV="pragma" CONTENT="no-cache">
 <meta HTTP-EQUIV="Cache-Control" CONTENT="no-store, must-revalidate">
 <meta HTTP-EQUIV="expires" CONTENT="0">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <title>中国电信智能网关</title>
  <link rel="shortcut icon" href="/luci-static/resources/image/favicon.ico">
  <link rel="bookmark" href="/luci-static/resources/image/favicon.ico">
  <link href="/luci-static/resources/css/login.css?version=5200" rel="stylesheet">
  <script src="/luci-static/resources/js/jquery.js?version=5200"></script>
  <script src="/luci-static/resources/js/util.js?version=5200"></script>
  <script src="/luci-static/resources/js/login.js?version=5200"></script>
  <script>

 window.onload =function() {console.log("The device support WiFi: " + 1);

 console.log("The device support USB: " + 1);

 console.log("The device type: " + 9);

 window.localStorage.setItem("hasWiFi", 1);
 window.localStorage.setItem("hasPots", 1);
 window.localStorage.setItem("hasUsb", 1);
 window.localStorage.setItem("hasMesh", 1);
 window.localStorage.setItem("devType", 9);
        }

        function hideHint()
        {
                $(".login-input").children(":last").remove();
                $("#login_username").removeAttr("disabled");
         $("#login_password").removeAttr("disabled");
        }
  </script>
  </head>
  <body onkeydown='keyCapscheck(event, 1)'>
  <div class="login_bg">
 <form method="post" id="argform">
         <input type="hidden" name="username" id="username" value="telecomadmin" />
         <input type="hidden" name="psd" id="psd" value="" />
         <input type="submit" style="display:none"/>
 </form><div class="logo"><img src="/luci-static/resources/image/logo_tianyi.png"
alt="logo"></div>
    <div class="line" id="line" name="line">
      <table align=left cellpadding=0 cellspace=0 border=0>
        <tr>
          <td id="line1" name="line1" valign="top">
          <img src="/luci-static/resources/image/line.png" style="opacity:0.2;">
        </td>
        <td id="line2" name="line2" valign="top">
          <img src="/luci-static/resources/image/line.png" style="margin-left:-3px;opacity:0.2;">
        </td>
        </tr>
      </table>
    </div>
    <script>
    if (bType == "IE8")
    {
         var speed=6;
         console.log("Current broswer is IE8.");
     function Marquee(){
       if(document.getElementById("line2").offsetWidth-
document.getElementById("line").scrollLeft<=0)
         document.getElementById("line").scrollLeft-
=document.getElementById("line1").offsetWidth;
       else{
```

```
          document.getElementById("line").scrollLeft++;
        }
      }
          setInterval(Marquee,speed);
        }
    </script>
    <div id='copyright_div'>
   Copyright (C) 2015        中国电信 All rights reserved.  
   <script>
          function isIPv6Addr(str)
                 {
                  return /:/.test(str) &&
                    str.match(/:/g).length<8 &&
                    /::/.test(str)
                    ?(str.match(/::/g).length==1 &&
                    /^::$|^(::)?([\da-f]{1,4}(:|::))*[\da-f]{1,4}(:|::)?$/i.test(str))
                    :/^([\da-f]{1,4}:){7}[\da-f]{1,4}$/i.test(str);
                 }

          if (isIPv6Addr(location.host))
                  var hosturl = "[" + location.host + "]";
          else
                  var hosturl = location
...
...
...
```

问题 2 / 5

TOC

“X-Content-Type-Options”头缺失或不安全	
严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1:8080/maintain
实体：	maintain (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

差异：

推理： AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值，这可能会更大程度地暴露于偷渡式下载攻击之下

测试请求和响应：

```
GET /maintain HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1/cgi-bin/luci
Connection: keep-alive
Host: 192.168.1.1:8080
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.0 200 OK
Connection: close
```

```
Server: HSANHomeGateway
Content-Length: 1582
Content-Type:

<!DOCTYPE html>
<html lang="en">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge">
 <meta name="viewport" content="width=device-width, initial-scale=1">
 <meta HTTP-EQUIV='Pragma' CONTENT='no-cache'>
 <title>       中国电信智能网关</title>
 <link href="/css/login.css?v=20250327153146" rel="stylesheet">
 <link href="/css/main_style.css?v=20250327153146" rel="stylesheet">
 <script src="/js/jquery.js?v=20250327153146"></script>
 <script src="/js/aes_1.js?v=20250327153146"></script>
 <script src="/js/common.js?v=20250327153146"></script>
  <script>
         var g_wlan24_num=8
         var g_wlan58_num=8
         var g_usb_num=1
         var g_province="JT"
  </script>
</head>
<body>
 <script>
     if (g_province == "JT" || g_province == "HAI") {
         window.location="/";
     } else {
         window.location="/register.html";
     }
 </script>       <div id="pop_window_div" style="display: none;"></div>
 <div id="pop_window_content_div" style="display: none;">
         <div id="pop_window_title"></div>
         <div id="pop_window_body">
                 <div id="pop_window_icon"></div>
                 <div id="pop_window_show_div">
                         <div id="pop_window_loading"></div>
                         <div id="pop_window_message"></div>
                         <div id="pop_window_option">
                                 <div id="pop_window_confirm" class="pop_window_action
bg_color_main">确认</div>
                                 <div id="pop_window_cancel" class="pop_window_action
bg_color_red">取消</div>
                         </div>
                 </div>
         </div>
 </div>
 <div id="loading" style="display: none;">
         <div id="loading_content">
                 <img src="/image/loading.gif">
         </div>
 </div>
</body>
</html>
```

问题 3 / 5

TOC

“X-Content-Type-Options”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1:8080/js/aes_1.js
实体：	aes_1.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

差异：

推理： AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值，这可能会更大程度地暴露于偷渡式下载攻击之下

测试请求和响应：

```
GET /js/aes_1.js?v=20250327153146 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1:8080/maintain
Connection: keep-alive
Host: 192.168.1.1:8080
Accept: */*
Accept-Language: en-US


HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 19061
Cache-control: public,max-age=86400
Content-Type: application/x-javascript

var passwd_key = ""
function encryted_pwd(pwd){
 var key = "";
 for(var i = 0; i < passwd_key.length; i++){
         if(passwd_key.charCodeAt(i) < 16){
                 key += ("0" + (passwd_key.charCodeAt(i)).toString(16));
                }
         else{
                 key += (passwd_key.charCodeAt(i)).toString(16);
                }
        }
 if (key.length > 64){
         key = key.slice(0,64);
        }
 else{
         for (var i = key.length; i < 64 ; i++){
                 key += "0";
                }
        }
 key = CryptoJS.enc.Hex.parse(key);
 return en_func(pwd,key);
}

var Crypto_aes_g_key = "6873616E000000000000000000000000000000000000000000000000000000000000000000000000";

function encrypt_info(pwd){
 var key = CryptoJS.enc.Hex.parse(Crypto_aes_g_key);
 return en_func(pwd,key);
}

function en_func(pwd,key){
 var ivRand = randNum(16);
 pwd = CryptoJS.enc.Utf8.parse(pwd);
```

```
 var encryptedPwd = CryptoJS.AES.encrypt(pwd, key, {
     //iv: CryptoJS.enc.Utf8.parse("0000000000000000"),
     iv: CryptoJS.enc.Hex.parse(ivRand),
     mode: CryptoJS.mode.CBC,
     padding: CryptoJS.pad.Pkcs7
 });

 var encryptedPwdStr = encryptedPwd.ciphertext.toString();
 //return encryptedBase64Str;
 var ivEncryptedPwd = ivRand + encryptedPwdStr;
 return ivEncryptedPwd;
}

function randNum(n){
    var rnd = "";
    var rndIv = "";
    for(var i=0;i<n;i++){
        rnd = Math.floor(Math.random()*256);
        if(rnd<16)
                rnd = "0" + rnd.toString(16);
         else
                rnd = rnd.toString(16);
         rndIv += rnd;
    }
    return rndIv;
}

function decrypt_info(encryptedIvPwd){
 var key = CryptoJS.enc.Hex.parse(Crypto_aes_g_key);
 var ivRecived = encryptedIvPwd.slice(0,32);
 var encryptedPwd = encryptedIvPwd.slice(32,encryptedIvPwd.length);
 var encryptedHexStr = CryptoJS.enc.Hex.parse(encryptedPwd);
    var encryptedBase64Str = CryptoJS.enc.Base64.stringify(encryptedHexStr);

    var decryptedData = CryptoJS.AES.decrypt(encryptedBase64Str, key, {
     //iv: CryptoJS.enc.Utf8.parse("0000000000000000"),
     iv: CryptoJS.enc.Hex.parse(ivRecived),
     mode: CryptoJS.mode.CBC,
     padding: CryptoJS.pad.Pkcs7
 });

    var decryptedStr = decryptedData.toString(CryptoJS.enc.Utf8);
    return decryptedStr.toString();
}

var hexMap = new Array('0', '1', '2', '3', '4', '5', '6', '7', '8', '9', 'A', 'B', 'C', 'D', 'E',
'F');

function getDHprvkey(){
 var dhPrvKey = "";
 dhPrvKey += (Math.floor(Math.random() * 15)).toString(16);
 for (var j = 0; j < 191; j++){
         dhPrvKey += (Math.floor(Math.random() * 16)).toString(16);
        }

 return dhPrvKey;
}

function getDHkey(g,n,p){
 var g_Bigint = Bigint.fromHex(g);
 var n_Bigint = Bigint.fromHex(n);
 var p_Bigint = Bigint.fromHex(p);
 var dhKey = Bigint._powmod(g_Bigint,n_Bigint,p_Bigint);
 var dhKey_binary = dhKey.toBinaryString();
 var dhKey_tmp = "";
 var tmp,tmpLen;
 for (var i=dhKey_binary.length-1; i >= 0; i=i-4){
         if ((i-3)<0){
                 tmp = dhKey_binary.slice(0,i+1);
                 tmpLen = 4 - tmp.length;
                 for (var j = 0; j < tmpLen; j++) {
                         tmp = "0" + tmp;
                        }
                }
         else
                 tmp = dhKey_binary.slice(i-3,i+1);
         dhKey_tmp = hexMap[((tmp[0]=='1')?8:0)+((tmp[1]=='1')?4:0)+((tmp[2]=='1')?2:0)+
((tmp[3]=='1')?1:0)] + dhKey_tmp;
```

```
        }
 if(dhKey_tmp.length % 2 == 1)
         dhKey_tmp = "0" + dhKey_tmp;
 return dhKey_tmp;
}

function genDHkey(data,privkey,p){
    data = eval("("+data+")");
 if(data.data.web_stuff){
          var keysuff = '', exclus = '', aeskey = '';
          keysuff = getDHkey(data.data.web_stuff, privkey, p);
          var hex1 = 0, hex2 = 0, hex3 = 0, dec = 0, len = keysuff.length/3;
          for(var i = 0; i < len; i+=2){
          hex1 = '0x'+keysuff.slice(i, i+2);
          hex2 = '0x'+keysuff.slice(i+len, i+len+2);
          hex3 = '0x'+keysuff.slice(i+2*len, i+2*len+2);
         dec = hex1 ^ hex2 ^ hex3;
         exclus = dec.toString(16);
         if(exclus.length < 2){
                         exclus = "0" + exclus;
                }
         aeskey += exclus;
     }
     Crypto_aes_g_key = aeskey;
        }
    else{
        Crypto_aes_g_key = "6873616E0000000000000000000000000000000000000000000000000000000000000000";
    }
}

var CryptoJS=CryptoJS||function(u,p){
 var d={},l=d.lib={},s=function(){},t=l.Base={extend:function(a){
                 s.prototype=this;
                 var c=new s;
                 a&&c.mixIn(a);
                 c.hasOwnProperty("init")||(c.init=function(){
                         c.$super.init.apply(this,arguments);
                 })       ;
                 c.init.prototype=c;
                 c.$super=this;
                 return c;
         }       ,
         create:function(){
                 var a=this.extend();
                 a.init.apply(a,arguments);
                 return a;
         }       ,
         init:function(){},
         mixIn:function(a){
                 for(var c in a)
                         a.hasOwnProperty(c)&&(this[c]=a[c]);
                 a.hasOwnProperty("toString")&&(this.toString=a.toString);
         }       ,
         clone:fun
...
...
...
```

问题 4 / 5

TOC

“X-Content-Type-Options”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1/luci-static/resources/js/util.js
实体：	util.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

差异：

推理： AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值，这可能会更大程度地暴露于偷渡式下载攻击之下

测试请求和响应：

```
GET /luci-static/resources/js/util.js?version=5200 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1/cgi-bin/luci
Connection: keep-alive
Host: 192.168.1.1
Accept: */*
Accept-Language: en-US


HTTP/1.1 200 OK
Last-Modified: Tue, 05 Mar 2024 01:09:21 GMT
Connection: Keep-Alive
Content-Length: 41626
Keep-Alive: timeout=20
ETag: "d6-a29a-65e670c1"
Date: Tue, 01 Apr 2025 01:20:48 GMT
Content-Type: text/javascript

var WEB_POLL_INTERVAL=5;

window.console = window.console || (function(){
    var c = {}; c.log = c.warn = c.debug = c.info = c.error = c.time = c.dir = c.profile
    = c.clear = c.exception = c.trace = c.assert = function(){};
    return c;
})();

var noWiFi = (window.localStorage.getItem("hasWiFi") == 1) ? 0 : 1;
var noPots = (window.localStorage.getItem("hasPots") == 1) ? 0 : 1;
var noUsb = (window.localStorage.getItem("hasUsb") == 1) ? 0 : 1;
var noMesh = (window.localStorage.getItem("hasMesh") == 1) ? 0 : 1;
var devType = window.localStorage.getItem("devType");

function isIE7Browser()
{
 if(navigator.appName == "Microsoft Internet Explorer" &&
navigator.appVersion.match(/7./i)=="7.")
 {
         return true;
        }
 else
        {
         return false;
        }
}
function judedNavation()
{
 if(navigator.appName == "Microsoft Internet Explorer" &&
navigator.appVersion.match(/6./i)=="6."){
         return 6;
```

```
 }
 else if(navigator.appName == "Microsoft Internet Explorer" &&
navigator.appVersion.match(/7./i)=="7."){
         return 7;
 }
 else if(navigator.appName == "Microsoft Internet Explorer" &&
navigator.appVersion.match(/8./i)=="8."){
         return 8;
 }
 else if(navigator.appName == "Microsoft Internet Explorer" &&
navigator.appVersion.match(/9./i)=="9."){
         return 9;
        }
 else{
         return 10;
        }
}


function createInput(id, name, placeholder, maxlength, type, value)
{
 var inputObj = "<input ";
 if ( id != "" && id != "undefined" )
        {
         inputObj += "id='" + id + "' ";
        }
 if ( name != "" && name != "undefined" )
        {
         inputObj += "name='" + name + "' ";
        }
 if ( placeholder != "" && placeholder != "undefined" )
        {
         inputObj += "placeholder='" + placeholder + "' ";
        }
 if ( maxlength != "" && maxlength != "undefined" )
        {
         inputObj += "maxlength='" + maxlength + "' ";
        }
 inputObj += "type='" + type + "' ";
 inputObj += "value='" + value + "' ";
 inputObj += ">";
 return inputObj;
}

function inputBindFocus()
{
 $("input[type='password'], .password_content input[type='text']").bind("focusin",
function(){
         $(this).parent().eq(0).addClass("password_content_focus");
         if ( !$(this).next().hasClass("password_switch_eyeon") )
                {
         $(this).next().addClass("password_switch_focus");
                }
 });
 $("input[type='password'], .password_content input[type='text']").bind("focusout",
function(){
         $(this).parent().eq(0).removeClass("password_content_focus");
         $(this).next().removeClass("password_switch_focus");
 });
}

function customSwitchInit()
{
 $(".switch_content").bind("click", function(){
         if($(this).hasClass("switch_content_on")){
                 $(this).removeClass("switch_content_on");
                 $(this).addClass("switch_content_off");
                 $(this).children("span").html("OFF ");
                 $("#" + $(this).attr("id") + "_value").val(0);
         }else{
                 $(this).addClass("switch_content_on");
                 $(this).removeClass("switch_content_off");
                 $(this).children("span").html(" ON");
                 $("#" + $(this).attr("id") + "_value").val(1);
                }
         console.log($("#" + $(this).attr("id") + "_value").val());
 });
}
```

```
function customSelectInit()
{
 $(".select-arrow").click(function(){
         $(this).parent().addClass("select-open");
        });

 //Èç¹ûÊó±êÏòÏÂ»¬¶¯£¬Ôò²»Òþ²Ø
 $(".dropdown-select").bind("mouseleave",
                 function(e)
                 {
                         var w = $(this).width();
                         var h = $(this).height();
                         var x = (e.pageX - this.offsetLeft - (w / 2)) * (w > h ? (h / w)
: 1);
                         var y = (e.pageY - this.offsetTop - (h / 2)) * (h > w ? (w / h) :
1);
                         var direction = Math.round((((Math.atan2(y, x) * (180 / Math.PI))
+ 180) / 90) + 3) % 4;
                         if(direction != 2)
                         {
                                 $(this).removeClass("select-open");
                                }
 });

 $(".dropdown-menu-select").mouseleave(function(){
        $(this).parent().removeClass("select-open");
 });

 $(".dropdown-menu-select li").click(function(){
         $(this).parent().siblings("label").first().text($(this).text());
         $("#" + $(this).parent().attr("id") + "_value").val($(this).attr("livalue"));
         $(this).parent().parent().removeClass("select-open");;
 });
}
function customPasswordInit()
{
 inputBindFocus();
 $(".password_switch").bind("click", function(){
         if( $(this).css("background-image").indexOf("eye_close") > -1 )
                {
                 $(this).removeClass("password_switch_unfocus");
                 $(this).removeClass("password_switch_focus");
                 $(this).addClass("password_switch_eyeon");
                }
         else
                {
                 $(this).removeClass("password_switch_eyeon");
                 $(this).addClass("password_switch_unfocus");
                }

         if( 9 > judedNavation() )
                {
                 var $pwdInput =
...
...
...
```

问题 5 / 5

TOC

“X-Content-Type-Options”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1:8080/js/common.js
实体：	common.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

差异：

推理： AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值，这可能会更大程度地暴露于偷渡式下载攻击之下

测试请求和响应：

```
GET /js/common.js?v=20250327153146 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1:8080/maintain
Connection: keep-alive
Host: 192.168.1.1:8080
Accept: */*
Accept-Language: en-US


HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 22938
Cache-control: public,max-age=86400
Content-Type: application/x-javascript

function web_server_result(s) {
 if (s == "null error") {
         return "        某些项的值无效，请重新填写"
 } else if (s == "data error") {
         return "        某些项的值无效，请重新填写"
 } else if (s == "set error") {
         return "        设置失败"
 } else if (s == "add error") {
         return "        添加失败"
 } else if (s == "del error") {
         return "        删除失败"
 } else if (s == "get error") {
         return "        获取配置失败"
 } else {
         return s
        }
}

function common_ajax_success(rsp, status, xhr) {
 var rsp_obj = rsp
 if (typeof(rsp) == "string")
         rsp_obj = JSON.parse(rsp)

 if (typeof(rsp_obj) == "object" && rsp_obj.retcode == "0" && rsp_obj.data.result ==
"SUCCESS") {
         location.reload()
 } else {
         var msg = ""
         if (rsp_obj.data && rsp_obj.data.errinfo) {
                 msg = msg + web_server_result(rsp_obj.data.errinfo)
                }
         if (rsp_obj.data && rsp_obj.data.result) {
                 msg = msg + rsp_obj.data.result
```

```
                }
         if (msg == "") {
                 msg = "       未知的错误"
                }

         pop_window.alert({title:"       警告", text:msg, confirm:true})
        }
}

function common_ajax_success_cb(rsp, status, xhr, cb) {
 var rsp_obj = rsp
 if (typeof(rsp) == "string")
         rsp_obj = JSON.parse(rsp)

 if (typeof(rsp_obj) == "object" && rsp_obj.retcode == "0" && rsp_obj.data.result ==
"SUCCESS") {
         cb()
 } else {
         var msg = ""
         if (rsp_obj.data && rsp_obj.data.errinfo) {
                 msg = msg + web_server_result(rsp_obj.data.errinfo)
                }
         if (rsp_obj.data && rsp_obj.data.result) {
                 msg = msg + rsp_obj.data.result
                }
         if (msg == "") {
                 msg = "       未知的错误"
                }

         pop_window.alert({title:"       警告", text:msg, confirm:true})
        }
}

function getQueryVariable(variable) {
    let query = window.location.search.substring(1);
    let vars = query.split("&");
    for (let i = 0; i < vars.length; i++) {
        let pair = vars[i].split("=");
        if (pair[0] == variable) {
          return pair[1];
        }
    }
}

function hasClass (ele, className) {
 var reg = new RegExp('(^|\\s)' + className + '(\\s|$)')
 return reg.test(ele.className)
}

function macToNumber(mac) {
 return Number("0x"+mac.replaceAll(':',''))
}

function ipToNumber(ip) {
 var num = 0;
 if(ip == "") {
         return num;
 }
    var aNum = ip.split(".");
    if(aNum.length != 4) {
        return num;
    }
    num += parseInt(aNum[0]) << 24;
    num += parseInt(aNum[1]) << 16;
    num += parseInt(aNum[2]) << 8;
    num += parseInt(aNum[3]) << 0;
    num = num >>> 0;//这个很关键，不然可能会出现负数的情况
    return num;
}

function numberToIp(number) {
    var ip = "";
    if(number <= 0) {
        return ip;
    }
    var ip3 = (number << 0 ) >>> 24;
    var ip2 = (number << 8 ) >>> 24;
    var ip1 = (number << 16) >>> 24;
```

```
    var ip0 = (number << 24) >>> 24

    ip += ip3 + "." + ip2 + "." + ip1 + "." + ip0;

    return ip;
}

function ipv4_prefix(ip) {
 var arr = ip.split('.')
 delete arr[3]
 return arr.join('.')
}

function is_ipv4(ip) {
 return /^(1\d{2}|2[0-4]\d|25[0-5]|[1-9]\d|[0-9])\.((1\d{2}|2[0-4]\d|25[0-5]|[1-
9]\d|\d)\.){2}(1\d{2}|2[0-4]\d|25[0-5]|[1-9]\d|\d)$/.test(ip)
}

function is_ipv6(ip) {
 return /^([\da-fA-F]{1,4}:){6}((25[0-5]|2[0-4]\d|[01]?\d\d?)\.){3}(25[0-5]|2[0-4]\d|[01]?
\d\d?)$|^::([\da-fA-F]{1,4}:){0,4}((25[0-5]|2[0-4]\d|[01]?\d\d?)\.){3}(25[0-5]|2[0-4]\d|[01]?
\d\d?)$|^([\da-fA-F]{1,4}:):([\da-fA-F]{1,4}:){0,3}((25[0-5]|2[0-4]\d|[01]?\d\d?)\.){3}(25[0-
5]|2[0-4]\d|[01]?\d\d?)$|^([\da-fA-F]{1,4}:){2}:([\da-fA-F]{1,4}:){0,2}((25[0-5]|2[0-4]\d|[01]?
\d\d?)\.){3}(25[0-5]|2[0-4]\d|[01]?\d\d?)$|^([\da-fA-F]{1,4}:){3}:([\da-fA-F]{1,4}:){0,1}((25[0-
5]|2[0-4]\d|[01]?\d\d?)\.){3}(25[0-5]|2[0-4]\d|[01]?\d\d?)$|^([\da-fA-F]{1,4}:){4}:((25[0-5]|2[0-
4]\d|[01]?\d\d?)\.){3}(25[0-5]|2[0-4]\d|[01]?\d\d?)$|^([\da-fA-F]{1,4}:){7}[\da-fA-F]{1,4}$|^:((:
[\da-fA-F]{1,4}){1,6}|:)$|^[\da-fA-F]{1,4}:((:[\da-fA-F]{1,4}){1,5}|:)$|^([\da-fA-F]{1,4}:){2}((:
[\da-fA-F]{1,4}){1,4}|:)$|^([\da-fA-F]{1,4}:){3}((:[\da-fA-F]{1,4}){1,3}|:)$|^([\da-fA-F]{1,4}:)
{4}((:[\da-fA-F]{1,4}){1,2}|:)$|^([\da-fA-F]{1,4}:){5}:([\da-fA-F]{1,4})?$|^([\da-fA-F]{1,4}:)
{6}:$/.test(ip)
}

function is_domain(domain) {
 return /^(?=^.{3,255}$)[a-zA-Z0-9][-a-zA-Z0-9]{0,62}(\.[a-zA-Z0-9][-a-zA-Z0-9]
{0,62})+$/.test(domain)
}

function is_hex(s) {
 for (var i in s) {
         if (!((s[i].charCodeAt() >= '0'.charCodeAt() && s[i].charCodeAt() <=
'9'.charCodeAt()) ||
                 (s[i].charCodeAt() >= 'a'.charCodeAt() && s[i].charCodeAt() <=
'f'.charCodeAt()) ||
                 (s[i].charCodeAt() >= 'A'.charCodeAt() && s[i].charCodeAt() <=
'F'.charCodeAt())))
                {
                 return false
                }
        }

 return true
}

function iform_data() {
    var data = {}
    $.each($("iform select:enabled"), function(i, select){
        data[select.name] = s
...
...
...
```

低 “X-XSS-Protection”头缺失或不安全 5 TOC

问题 1 / 5 TOC

“X-XSS-Protection”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1/
实体：	(Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

差异：

推理： AppScan 检测到 X-XSS-Protection 响应头缺失或具有不安全值，这可能会造成跨站点脚本编制攻击

测试请求和响应：

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: 192.168.1.1
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Last-Modified: Thu, 10 Nov 2022 02:15:45 GMT
Connection: Keep-Alive
Content-Length: 444
X-Frame-Options: SAMEORIGIN
Keep-Alive: timeout=20
ETag: "15a-1bc-636c5ed1"
Date: Tue, 01 Apr 2025 01:20:47 GMT
Content-Type: text/html

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=Edge">
<meta http-equiv="refresh" content="0; URL=/cgi-bin/luci" />
<meta HTTP-EQUIV="pragma" CONTENT="no-cache">
<meta HTTP-EQUIV="Cache-Control" CONTENT="no-store, must-revalidate">
<meta HTTP-EQUIV="expires" CONTENT="0">
<title>中国电信智能网关</title>

</head>
<body>
</body>
</html>


GET /cgi-bin/luci HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1/
Connection: Keep-Alive
Host: 192.168.1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Transfer-Encoding: chunked
Connection: Keep-Alive
```

```
X-Frame-Options: SAMEORIGIN
X-Frame-Options: SAMEORIGIN
Keep-Alive: timeout=20
Cache-Control: no-cache
Expires: 0
Content-Type: text/html; charset=utf-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>
  <head>
  <meta http-equiv='Content-Type' content='text/html; charset=utf-8'/>
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
 <meta HTTP-EQUIV="pragma" CONTENT="no-cache">
 <meta HTTP-EQUIV="Cache-Control" CONTENT="no-store, must-revalidate">
 <meta HTTP-EQUIV="expires" CONTENT="0">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <title>中国电信智能网关</title>
  <link rel="shortcut icon" href="/luci-static/resources/image/favicon.ico">
  <link rel="bookmark" href="/luci-static/resources/image/favicon.ico">
  <link href="/luci-static/resources/css/login.css?version=5200" rel="stylesheet">
  <script src="/luci-static/resources/js/jquery.js?version=5200"></script>
  <script src="/luci-static/resources/js/util.js?version=5200"></script>
  <script src="/luci-static/resources/js/login.js?version=5200"></script>
  <script>

 window.onload =function() {console.log("The device support WiFi: " + 1);

 console.log("The device support USB: " + 1);

 console.log("The device type: " + 9);

 window.localStorage.setItem("hasWiFi", 1);
 window.localStorage.setItem("hasPots", 1);
 window.localStorage.setItem("hasUsb", 1);
 window.localStorage.setItem("hasMesh", 1);
 window.localStorage.setItem("devType", 9);
        }

        function hideHint()
        {
                $(".login-input").children(":last").remove();
                $("#login_username").removeAttr("disabled");
         $("#login_password").removeAttr("disabled");
        }
  </script>
  </head>
  <body onkeydown='keyCapscheck(event, 1)'>
  <div class="login_bg">
 <form method="post" id="argform">
         <input type="hidden" name="username" id="username" value="telecomadmin" />
         <input type="hidden" name="psd" id="psd" value="" />
         <input type="submit" style="display:none"/>
 </form><div class="logo"><img src="/luci-static/resources/image/logo_tianyi.png"
alt="logo"></div>
    <div class="line" id="line" name="line">
      <table align=left cellpadding=0 cellspace=0 border=0>
        <tr>
          <td id="line1" name="line1" valign="top">
          <img src="/luci-static/resources/image/line.png" style="opacity:0.2;">
        </td>
        <td id="line2" name="line2" valign="top">
          <img src="/luci-static/resources/image/line.png" style="margin-left:-3px;opacity:0.2;">
        </td>
        </tr>
      </table>
    </div>
    <script>
    if (bType == "IE8")
    {
         var speed=6;
         console.log("Current broswer is IE8.");
     function Marquee(){
       if(document.getElementById("line2").offsetWidth-
document.getElementById("line").scrollLeft<=0)
         document.getElementById("line").scrollLeft-
=document.getElementById("line1").offsetWidth;
       else{
```

```
          document.getElementById("line").scrollLeft++;
        }
      }
          setInterval(Marquee,speed);
        }
    </script>
    <div id='copyright_div'>
   Copyright (C) 2015        中国电信 All rights reserved.  
   <script>
          function isIPv6Addr(str)
                 {
                  return /:/.test(str) &&
                    str.match(/:/g).length<8 &&
                    /::/.test(str)
                    ?(str.match(/::/g).length==1 &&
                    /^::$|^(::)?([\da-f]{1,4}(:|::))*[\da-f]{1,4}(:|::)?$/i.test(str))
                    :/^([\da-f]{1,4}:){7}[\da-f]{1,4}$/i.test(str);
                 }

          if (isIPv6Addr(location.host))
                  var hosturl = "[" + location.
...
...
...
```

问题 2 / 5

TOC

“X-XSS-Protection”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1:8080/maintain
实体：	maintain (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

差异：

推理： AppScan 检测到 X-XSS-Protection 响应头缺失或具有不安全值，这可能会造成跨站点脚本编制攻击

测试请求和响应：

```
GET /maintain HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1/cgi-bin/luci
Connection: keep-alive
Host: 192.168.1.1:8080
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 1582
```

```
Content-Type:

<!DOCTYPE html>
<html lang="en">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge">
 <meta name="viewport" content="width=device-width, initial-scale=1">
 <meta HTTP-EQUIV='Pragma' CONTENT='no-cache'>
 <title>       中国电信智能网关</title>
 <link href="/css/login.css?v=20250327153146" rel="stylesheet">
 <link href="/css/main_style.css?v=20250327153146" rel="stylesheet">
 <script src="/js/jquery.js?v=20250327153146"></script>
 <script src="/js/aes_1.js?v=20250327153146"></script>
 <script src="/js/common.js?v=20250327153146"></script>
  <script>
         var g_wlan24_num=8
         var g_wlan58_num=8
         var g_usb_num=1
         var g_province="JT"
  </script>
</head>
<body>
 <script>
     if (g_province == "JT" || g_province == "HAI") {
         window.location="/";
     } else {
         window.location="/register.html";
     }
 </script>       <div id="pop_window_div" style="display: none;"></div>
 <div id="pop_window_content_div" style="display: none;">
         <div id="pop_window_title"></div>
         <div id="pop_window_body">
                 <div id="pop_window_icon"></div>
                 <div id="pop_window_show_div">
                         <div id="pop_window_loading"></div>
                         <div id="pop_window_message"></div>
                         <div id="pop_window_option">
                                 <div id="pop_window_confirm" class="pop_window_action
bg_color_main">确认</div>
                                 <div id="pop_window_cancel" class="pop_window_action
bg_color_red">取消</div>
                         </div>
                 </div>
         </div>
 </div>
 <div id="loading" style="display: none;">
         <div id="loading_content">
                 <img src="/image/loading.gif">
         </div>
 </div>
</body>
</html>
```

问题 3 / 5

TOC

“X-XSS-Protection”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1:8080/js/aes_1.js
实体：	aes_1.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

差异：

推理： AppScan 检测到 X-XSS-Protection 响应头缺失或具有不安全值，这可能会造成跨站点脚本编制攻击

测试请求和响应：

```
GET /js/aes_1.js?v=20250327153146 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1:8080/maintain
Connection: keep-alive
Host: 192.168.1.1:8080
Accept: */*
Accept-Language: en-US


HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 19061
Cache-control: public,max-age=86400
Content-Type: application/x-javascript

var passwd_key = ""
function encryted_pwd(pwd){
 var key = "";
 for(var i = 0; i < passwd_key.length; i++){
         if(passwd_key.charCodeAt(i) < 16){
                 key += ("0" + (passwd_key.charCodeAt(i)).toString(16));
                }
         else{
                 key += (passwd_key.charCodeAt(i)).toString(16);
                }
        }
 if (key.length > 64){
         key = key.slice(0,64);
        }
 else{
         for (var i = key.length; i < 64 ; i++){
                 key += "0";
                }
        }
 key = CryptoJS.enc.Hex.parse(key);
 return en_func(pwd,key);
}

var Crypto_aes_g_key = "6873616E000000000000000000000000000000000000000000000000000000000000000000000000";

function encrypt_info(pwd){
 var key = CryptoJS.enc.Hex.parse(Crypto_aes_g_key);
 return en_func(pwd,key);
}

function en_func(pwd,key){
 var ivRand = randNum(16);
 pwd = CryptoJS.enc.Utf8.parse(pwd);
```

```
 var encryptedPwd = CryptoJS.AES.encrypt(pwd, key, {
     //iv: CryptoJS.enc.Utf8.parse("0000000000000000"),
     iv: CryptoJS.enc.Hex.parse(ivRand),
     mode: CryptoJS.mode.CBC,
     padding: CryptoJS.pad.Pkcs7
 });

 var encryptedPwdStr = encryptedPwd.ciphertext.toString();
 //return encryptedBase64Str;
 var ivEncryptedPwd = ivRand + encryptedPwdStr;
 return ivEncryptedPwd;
}

function randNum(n){
    var rnd = "";
    var rndIv = "";
    for(var i=0;i<n;i++){
        rnd = Math.floor(Math.random()*256);
        if(rnd<16)
                rnd = "0" + rnd.toString(16);
         else
                rnd = rnd.toString(16);
         rndIv += rnd;
    }
    return rndIv;
}

function decrypt_info(encryptedIvPwd){
 var key = CryptoJS.enc.Hex.parse(Crypto_aes_g_key);
 var ivRecived = encryptedIvPwd.slice(0,32);
 var encryptedPwd = encryptedIvPwd.slice(32,encryptedIvPwd.length);
 var encryptedHexStr = CryptoJS.enc.Hex.parse(encryptedPwd);
    var encryptedBase64Str = CryptoJS.enc.Base64.stringify(encryptedHexStr);

    var decryptedData = CryptoJS.AES.decrypt(encryptedBase64Str, key, {
     //iv: CryptoJS.enc.Utf8.parse("0000000000000000"),
     iv: CryptoJS.enc.Hex.parse(ivRecived),
     mode: CryptoJS.mode.CBC,
     padding: CryptoJS.pad.Pkcs7
 });

    var decryptedStr = decryptedData.toString(CryptoJS.enc.Utf8);
    return decryptedStr.toString();
}

var hexMap = new Array('0', '1', '2', '3', '4', '5', '6', '7', '8', '9', 'A', 'B', 'C', 'D', 'E',
'F');

function getDHprvkey(){
 var dhPrvKey = "";
 dhPrvKey += (Math.floor(Math.random() * 15)).toString(16);
 for (var j = 0; j < 191; j++){
         dhPrvKey += (Math.floor(Math.random() * 16)).toString(16);
        }

 return dhPrvKey;
}

function getDHkey(g,n,p){
 var g_Bigint = Bigint.fromHex(g);
 var n_Bigint = Bigint.fromHex(n);
 var p_Bigint = Bigint.fromHex(p);
 var dhKey = Bigint._powmod(g_Bigint,n_Bigint,p_Bigint);
 var dhKey_binary = dhKey.toBinaryString();
 var dhKey_tmp = "";
 var tmp,tmpLen;
 for (var i=dhKey_binary.length-1; i >= 0; i=i-4){
         if ((i-3)<0){
                 tmp = dhKey_binary.slice(0,i+1);
                 tmpLen = 4 - tmp.length;
                 for (var j = 0; j < tmpLen; j++) {
                         tmp = "0" + tmp;
                        }
                }
         else
                 tmp = dhKey_binary.slice(i-3,i+1);
         dhKey_tmp = hexMap[((tmp[0]=='1')?8:0)+((tmp[1]=='1')?4:0)+((tmp[2]=='1')?2:0)+
((tmp[3]=='1')?1:0)] + dhKey_tmp;
```

```
        }
 if(dhKey_tmp.length % 2 == 1)
         dhKey_tmp = "0" + dhKey_tmp;
 return dhKey_tmp;
}

function genDHkey(data,privkey,p){
    data = eval("("+data+")");
 if(data.data.web_stuff){
          var keysuff = '', exclus = '', aeskey = '';
          keysuff = getDHkey(data.data.web_stuff, privkey, p);
          var hex1 = 0, hex2 = 0, hex3 = 0, dec = 0, len = keysuff.length/3;
          for(var i = 0; i < len; i+=2){
          hex1 = '0x'+keysuff.slice(i, i+2);
          hex2 = '0x'+keysuff.slice(i+len, i+len+2);
          hex3 = '0x'+keysuff.slice(i+2*len, i+2*len+2);
         dec = hex1 ^ hex2 ^ hex3;
         exclus = dec.toString(16);
         if(exclus.length < 2){
                         exclus = "0" + exclus;
                }
         aeskey += exclus;
     }
     Crypto_aes_g_key = aeskey;
        }
    else{
        Crypto_aes_g_key = "6873616E0000000000000000000000000000000000000000000000000000000000000000";
    }
}

var CryptoJS=CryptoJS||function(u,p){
 var d={},l=d.lib={},s=function(){},t=l.Base={extend:function(a){
                s.prototype=this;
                var c=new s;
                a&&c.mixIn(a);
                c.hasOwnProperty("init")||(c.init=function(){
                        c.$super.init.apply(this,arguments);
                })       ;
                c.init.prototype=c;
                c.$super=this;
                return c;
         }       ,
         create:function(){
                var a=this.extend();
                a.init.apply(a,arguments);
                return a;
         }       ,
         init:function(){},
         mixIn:function(a){
                for(var c in a)
                        a.hasOwnProperty(c)&&(this[c]=a[c]);
                a.hasOwnProperty("toString")&&(this.toString=a.toString);
         }       ,
         clone:fun
...
...
...
```

问题 4 / 5

TOC

“X-XSS-Protection”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1/luci-static/resources/js/util.js
实体：	util.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

差异：

推理： AppScan 检测到 X-XSS-Protection 响应头缺失或具有不安全值，这可能会造成跨站点脚本编制攻击

测试请求和响应：

```
GET /luci-static/resources/js/util.js?version=5200 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1/cgi-bin/luci
Connection: keep-alive
Host: 192.168.1.1
Accept: */*
Accept-Language: en-US


HTTP/1.1 200 OK
Last-Modified: Tue, 05 Mar 2024 01:09:21 GMT
Connection: Keep-Alive
Content-Length: 41626
Keep-Alive: timeout=20
ETag: "d6-a29a-65e670c1"
Date: Tue, 01 Apr 2025 01:20:48 GMT
Content-Type: text/javascript

var WEB_POLL_INTERVAL=5;

window.console = window.console || (function(){
    var c = {}; c.log = c.warn = c.debug = c.info = c.error = c.time = c.dir = c.profile
    = c.clear = c.exception = c.trace = c.assert = function(){};
    return c;
})();

var noWiFi = (window.localStorage.getItem("hasWiFi") == 1) ? 0 : 1;
var noPots = (window.localStorage.getItem("hasPots") == 1) ? 0 : 1;
var noUsb = (window.localStorage.getItem("hasUsb") == 1) ? 0 : 1;
var noMesh = (window.localStorage.getItem("hasMesh") == 1) ? 0 : 1;
var devType = window.localStorage.getItem("devType");

function isIE7Browser()
{
 if(navigator.appName == "Microsoft Internet Explorer" &&
navigator.appVersion.match(/7./i)=="7.")
 {
         return true;
        }
 else
        {
         return false;
        }
}
function judedNavation()
{
 if(navigator.appName == "Microsoft Internet Explorer" &&
navigator.appVersion.match(/6./i)=="6."){
         return 6;
```

```
 }
 else if(navigator.appName == "Microsoft Internet Explorer" &&
navigator.appVersion.match(/7./i)=="7."){
         return 7;
 }
 else if(navigator.appName == "Microsoft Internet Explorer" &&
navigator.appVersion.match(/8./i)=="8."){
         return 8;
 }
 else if(navigator.appName == "Microsoft Internet Explorer" &&
navigator.appVersion.match(/9./i)=="9."){
         return 9;
        }
 else{
         return 10;
        }
}


function createInput(id, name, placeholder, maxlength, type, value)
{
 var inputObj = "<input ";
 if ( id != "" && id != "undefined" )
        {
         inputObj += "id='" + id + "' ";
        }
 if ( name != "" && name != "undefined" )
        {
         inputObj += "name='" + name + "' ";
        }
 if ( placeholder != "" && placeholder != "undefined" )
        {
         inputObj += "placeholder='" + placeholder + "' ";
        }
 if ( maxlength != "" && maxlength != "undefined" )
        {
         inputObj += "maxlength='" + maxlength + "' ";
        }
 inputObj += "type='" + type + "' ";
 inputObj += "value='" + value + "' ";
 inputObj += ">";
 return inputObj;
}

function inputBindFocus()
{
 $("input[type='password'], .password_content input[type='text']").bind("focusin",
function(){
         $(this).parent().eq(0).addClass("password_content_focus");
         if ( !$(this).next().hasClass("password_switch_eyeon") )
                {
         $(this).next().addClass("password_switch_focus");
                }
 });
 $("input[type='password'], .password_content input[type='text']").bind("focusout",
function(){
         $(this).parent().eq(0).removeClass("password_content_focus");
         $(this).next().removeClass("password_switch_focus");
 });
}

function customSwitchInit()
{
 $(".switch_content").bind("click", function(){
         if($(this).hasClass("switch_content_on")){
                 $(this).removeClass("switch_content_on");
                 $(this).addClass("switch_content_off");
                 $(this).children("span").html("OFF ");
                 $("#" + $(this).attr("id") + "_value").val(0);
         }else{
                 $(this).addClass("switch_content_on");
                 $(this).removeClass("switch_content_off");
                 $(this).children("span").html(" ON");
                 $("#" + $(this).attr("id") + "_value").val(1);
                }
         console.log($("#" + $(this).attr("id") + "_value").val());
 });
}
```

```
function customSelectInit()
{
 $(".select-arrow").click(function(){
         $(this).parent().addClass("select-open");
        });

 //È¢¹ûÊó±êÏòÏÂ»¬¶¯£¬Ôò²»Òþ²Ø
 $(".dropdown-select").bind("mouseleave",
                 function(e)
                 {
                         var w = $(this).width();
                         var h = $(this).height();
                         var x = (e.pageX - this.offsetLeft - (w / 2)) * (w > h ? (h / w)
: 1);
                         var y = (e.pageY - this.offsetTop - (h / 2)) * (h > w ? (w / h) :
1);
                         var direction = Math.round((((Math.atan2(y, x) * (180 / Math.PI))
+ 180) / 90) + 3) % 4;
                         if(direction != 2)
                         {
                                 $(this).removeClass("select-open");
                                }
 });

 $(".dropdown-menu-select").mouseleave(function(){
        $(this).parent().removeClass("select-open");
 });

 $(".dropdown-menu-select li").click(function(){
         $(this).parent().siblings("label").first().text($(this).text());
         $("#" + $(this).parent().attr("id") + "_value").val($(this).attr("livalue"));
         $(this).parent().parent().removeClass("select-open");;
 });
}
function customPasswordInit()
{
 inputBindFocus();
 $(".password_switch").bind("click", function(){
         if( $(this).css("background-image").indexOf("eye_close") > -1 )
                {
                 $(this).removeClass("password_switch_unfocus");
                 $(this).removeClass("password_switch_focus");
                 $(this).addClass("password_switch_eyeon");
                }
         else
                {
                 $(this).removeClass("password_switch_eyeon");
                 $(this).addClass("password_switch_unfocus");
                }

         if( 9 > judedNavation() )
                {
                 var $pwdInput =
...
...
...
```

问题 5 / 5

TOC

“X-XSS-Protection”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1:8080/js/common.js
实体：	common.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

差异：

推理： AppScan 检测到 X-XSS-Protection 响应头缺失或具有不安全值，这可能会造成跨站点脚本编制攻击

测试请求和响应：

```
GET /js/common.js?v=20250327153146 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1:8080/maintain
Connection: keep-alive
Host: 192.168.1.1:8080
Accept: */*
Accept-Language: en-US


HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 22938
Cache-control: public,max-age=86400
Content-Type: application/x-javascript

function web_server_result(s) {
 if (s == "null error") {
         return "        某些项的值无效，请重新填写"
 } else if (s == "data error") {
         return "        某些项的值无效，请重新填写"
 } else if (s == "set error") {
         return "        设置失败"
 } else if (s == "add error") {
         return "        添加失败"
 } else if (s == "del error") {
         return "        删除失败"
 } else if (s == "get error") {
         return "        获取配置失败"
 } else {
         return s
        }
}

function common_ajax_success(rsp, status, xhr) {
 var rsp_obj = rsp
 if (typeof(rsp) == "string")
         rsp_obj = JSON.parse(rsp)

 if (typeof(rsp_obj) == "object" && rsp_obj.retcode == "0" && rsp_obj.data.result ==
"SUCCESS") {
         location.reload()
 } else {
         var msg = ""
         if (rsp_obj.data && rsp_obj.data.errinfo) {
                 msg = msg + web_server_result(rsp_obj.data.errinfo)
                }
         if (rsp_obj.data && rsp_obj.data.result) {
                 msg = msg + rsp_obj.data.result
```

```
                }
         if (msg == "") {
                 msg = "       未知的错误"
                }

         pop_window.alert({title:"       警告", text:msg, confirm:true})
        }
}

function common_ajax_success_cb(rsp, status, xhr, cb) {
 var rsp_obj = rsp
 if (typeof(rsp) == "string")
         rsp_obj = JSON.parse(rsp)

 if (typeof(rsp_obj) == "object" && rsp_obj.retcode == "0" && rsp_obj.data.result ==
"SUCCESS") {
         cb()
 } else {
         var msg = ""
         if (rsp_obj.data && rsp_obj.data.errinfo) {
                 msg = msg + web_server_result(rsp_obj.data.errinfo)
                }
         if (rsp_obj.data && rsp_obj.data.result) {
                 msg = msg + rsp_obj.data.result
                }
         if (msg == "") {
                 msg = "       未知的错误"
                }

         pop_window.alert({title:"       警告", text:msg, confirm:true})
        }
}

function getQueryVariable(variable) {
    let query = window.location.search.substring(1);
    let vars = query.split("&");
    for (let i = 0; i < vars.length; i++) {
        let pair = vars[i].split("=");
        if (pair[0] == variable) {
          return pair[1];
        }
    }
}

function hasClass (ele, className) {
 var reg = new RegExp('(^|\\s)' + className + '(\\s|$)')
 return reg.test(ele.className)
}

function macToNumber(mac) {
 return Number("0x"+mac.replaceAll(':',''))
}

function ipToNumber(ip) {
 var num = 0;
 if(ip == "") {
         return num;
 }
    var aNum = ip.split(".");
    if(aNum.length != 4) {
        return num;
    }
    num += parseInt(aNum[0]) << 24;
    num += parseInt(aNum[1]) << 16;
    num += parseInt(aNum[2]) << 8;
    num += parseInt(aNum[3]) << 0;
    num = num >>> 0;//这个很关键，不然可能会出现负数的情况
    return num;
}

function numberToIp(number) {
    var ip = "";
    if(number <= 0) {
        return ip;
    }
    var ip3 = (number << 0 ) >>> 24;
    var ip2 = (number << 8 ) >>> 24;
    var ip1 = (number << 16) >>> 24;
```

```
    var ip0 = (number << 24) >>> 24

    ip += ip3 + "." + ip2 + "." + ip1 + "." + ip0;

    return ip;
}

function ipv4_prefix(ip) {
 var arr = ip.split('.')
 delete arr[3]
 return arr.join('.')
}

function is_ipv4(ip) {
 return /^(1\d{2}|2[0-4]\d|25[0-5]|[1-9]\d|[0-9])\.((1\d{2}|2[0-4]\d|25[0-5]|[1-
9]\d|\d)\.){2}(1\d{2}|2[0-4]\d|25[0-5]|[1-9]\d|\d)$/.test(ip)
}

function is_ipv6(ip) {
 return /^([\da-fA-F]{1,4}:){6}((25[0-5]|2[0-4]\d|[01]?\d\d?)\.){3}(25[0-5]|2[0-4]\d|[01]?
\d\d?)$|^::([\da-fA-F]{1,4}:){0,4}((25[0-5]|2[0-4]\d|[01]?\d\d?)\.){3}(25[0-5]|2[0-4]\d|[01]?
\d\d?)$|^([\da-fA-F]{1,4}:):([\da-fA-F]{1,4}:){0,3}((25[0-5]|2[0-4]\d|[01]?\d\d?)\.){3}(25[0-
5]|2[0-4]\d|[01]?\d\d?)$|^([\da-fA-F]{1,4}:){2}:([\da-fA-F]{1,4}:){0,2}((25[0-5]|2[0-4]\d|[01]?
\d\d?)\.){3}(25[0-5]|2[0-4]\d|[01]?\d\d?)$|^([\da-fA-F]{1,4}:){3}:([\da-fA-F]{1,4}:){0,1}((25[0-
5]|2[0-4]\d|[01]?\d\d?)\.){3}(25[0-5]|2[0-4]\d|[01]?\d\d?)$|^([\da-fA-F]{1,4}:){4}:((25[0-5]|2[0-
4]\d|[01]?\d\d?)\.){3}(25[0-5]|2[0-4]\d|[01]?\d\d?)$|^([\da-fA-F]{1,4}:){7}[\da-fA-F]{1,4}$|^:((:
[\da-fA-F]{1,4}){1,6}|:)$|^[\da-fA-F]{1,4}:((:[\da-fA-F]{1,4}){1,5}|:)$|^([\da-fA-F]{1,4}:){2}((:
[\da-fA-F]{1,4}){1,4}|:)$|^([\da-fA-F]{1,4}:){3}((:[\da-fA-F]{1,4}){1,3}|:)$|^([\da-fA-F]{1,4}:)
{4}((:[\da-fA-F]{1,4}){1,2}|:)$|^([\da-fA-F]{1,4}:){5}:([\da-fA-F]{1,4})?$|^([\da-fA-F]{1,4}:)
{6}:$/.test(ip)
}

function is_domain(domain) {
 return /^(?=^.{3,255}$)[a-zA-Z0-9][-a-zA-Z0-9]{0,62}(\.[a-zA-Z0-9][-a-zA-Z0-9]
{0,62})+$/.test(domain)
}

function is_hex(s) {
 for (var i in s) {
         if (!((s[i].charCodeAt() >= '0'.charCodeAt() && s[i].charCodeAt() <=
'9'.charCodeAt()) ||
                 (s[i].charCodeAt() >= 'a'.charCodeAt() && s[i].charCodeAt() <=
'f'.charCodeAt()) ||
                 (s[i].charCodeAt() >= 'A'.charCodeAt() && s[i].charCodeAt() <=
'F'.charCodeAt())))
                {
                 return false
                }
        }

 return true
}

function iform_data() {
    var data = {}
    $.each($("iform select:enabled"), function(i, select){
        data[select.name] = s
...
...
...
```

低 查询中接受的主体参数 1 TOC

问题 1 / 1 TOC

查询中接受的主体参数

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1:8080/boaform/web_login_exe.cgi
实体：	web_login_exe.cgi (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	请勿接受在查询字符串中发送的主体参数

差异： **主体参数** 已从请求除去：
查询参数 已添加至请求：
主体参数 已从请求除去： `eda7688a7f9fdb14bd1e592df15fe5879bb8439cf139555eb174a47639ac085b`
查询参数 已添加至请求： `eda7688a7f9fdb14bd1e592df15fe5879bb8439cf139555eb174a47639ac085b`
方法 从以下位置进行控制： `POST` 至： `GET`

推理： 测试结果似乎指示存在脆弱性，因为“测试响应”与“原始响应”类似，这表明应用程序处理了查询总提交的主体参数。

测试请求和响应：

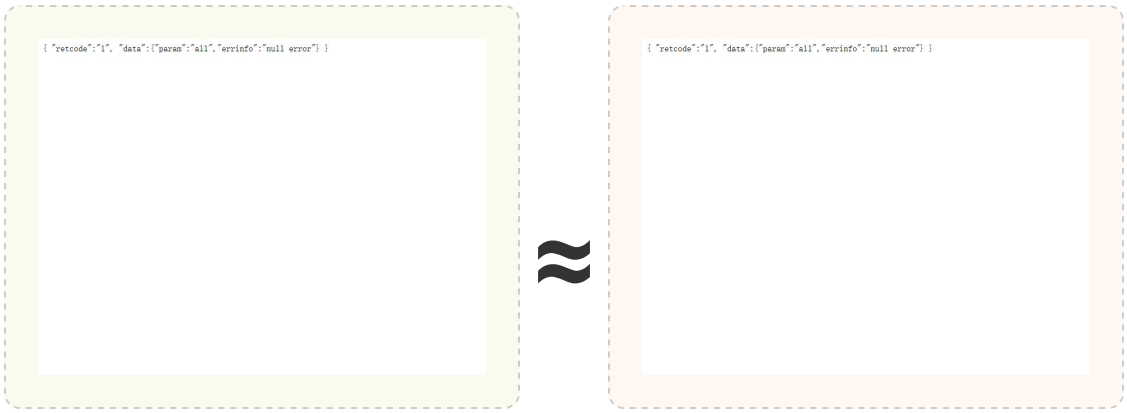
```
POST /boaform/web_login_exe.cgi HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1:8080/login.html
Cookie:
Connection: keep-alive
Host: 192.168.1.1:8080
Cache-Control: no-cache
Accept: */*
Origin: http://192.168.1.1:8080
Accept-Language: en-US
content-type: application/x-www-form-urlencoded

web_login_name=&web_login_password=eda7688a7f9fdb14bd1e592df15fe5879bb8439cf139555eb174a47639ac085b

HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 72
Content-Type: text/html

{
    "retcode":"1",
    "data":{"param":"all","errinfo":"null error"}
}
```

原始响应 **测试响应**


{ "retcode":"1", "data":{"param":"all","errinfo":"null error"} }
≈
{ "retcode":"1", "data":{"param":"all","errinfo":"null error"} }

参 HTML 注释敏感信息泄露 1 TOC

问题 1 / 1 TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://192.168.1.1/cgi-bin/luci
实体：	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtm... (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /cgi-bin/luci HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1/
Connection: Keep-Alive
Host: 192.168.1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Transfer-Encoding: chunked
Connection: Keep-Alive
X-Frame-Options: SAMEORIGIN
X-Frame-Options: SAMEORIGIN
Keep-Alive: timeout=20
Cache-Control: no-cache
Expires: 0
Content-Type: text/html; charset=utf-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>
  <head>
  <meta http-equiv='Content-Type' content='text/html; charset=utf-8'/>
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
 <meta HTTP-EQUIV="pragma" CONTENT="no-cache">
 <meta HTTP-EQUIV="Cache-Control" CONTENT="no-store, must-revalidate">
 <meta HTTP-EQUIV="expires" CONTENT="0">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <title>中国电信智能网关</title>
  <link rel="shortcut icon" href="/luci-static/resources/image/favicon.ico">
```

```
  <link rel="bookmark" href="/luci-static/resources/image/favicon.ico">
  <link href="/luci-static/resources/css/login.css?version=5200" rel="stylesheet">
  <script src="/luci-static/resources/js/jquery.js?version=5200"></script>
  <script src="/luci-static/resources/js/util.js?version=5200"></script>
  <script src="/luci-static/resources/js/login.js?version=5200"></script>
  <script>

 window.onload =function() {console.log("The device support WiFi: " + 1);

 console.log("The device support USB: " + 1);

 console.log("The device type: " + 9);

 window.localStorage.setItem("hasWiFi", 1);
 window.localStorage.setItem("hasPots", 1);
 window.localStorage.setItem("hasUsb", 1);
 window.localStorage.setItem("hasMesh", 1);
 window.localStorage.setItem("devType", 9);
        }

        function hideHint()
        {
                $(".login-input").children(":last").remove();
                $("#login_username").removeAttr("disabled");
         $("#login_password").removeAttr("disabled");
        }
  </script>
  </head>
  <body onkeydown='keyCapscheck(event, 1)'>
  <div class="login_bg">
 <form method="post" id="argform">
         <input type="hidden" name="username" id="username" value="telecomadmin" />
         <input type="hidden" name="psd" id="psd" value="" />
         <input type="submit" style="display:none"/>
 </form><div class="logo"><img src="/luci-static/resources/image/logo_tianyi.png"
alt="logo"></div>
    <div class="line" id="line" name="line">
      <table align=left cellpadding=0 cellspace=0 border=0>
        <tr>
          <td id="line1" name="line1" valign="top">
          <img src="/luci-static/resources/image/line.png" style="opacity:0.2;">
        </td>
        <td id="line2" name="line2" valign="top">
          <img src="/luci-static/resources/image/line.png" style="margin-left:-3px;opacity:0.2;">
        </td>
        </tr>
      </table>
    </div>
    <script>
    if (bType == "IE8")
    {
         var speed=6;
         console.log("Current broswer is IE8.");
     function Marquee(){
       if(document.getElementById("line2").offsetWidth-
document.getElementById("line").scrollLeft<=0)
         document.getElementById("line").scrollLeft-
=document.getElementById("line1").offsetWidth;
       else{
         document.getElementById("line").scrollLeft++;
       }
     }
         setInterval(Marquee,speed);
        }
    </script>
    <div id='copyright_div'>
   Copyright (C) 2015        中国电信 All rights reserved.  
   <script>
         function isIPv6Addr(str)
                {
                 return /:/.test(str) &&
                   str.match(/:/g).length<8 &&
                   /::/.test(str)
                   ?(str.match(/::/g).length==1 &&
                   /^::$|^(::)?([\da-f]{1,4}(:|::))*[\da-f]{1,4}(:|::)?$/i.test(str))
                   :/^([\da-f]{1,4}:){7}[\da-f]{1,4}$/i.test(str);
                }
```

```
          if (isIPv6Addr(location.host))
                  var hosturl = "[" + location.host + "]";
          else
                  var hosturl = location.host;

                document.write("<a href='" + location.protocol + "//" + hosturl +
":8080/maintain" + "'>快速装维入口</a>");
   </script>
 </div>
  </div>

  <div class="container-fluid login_block">
    <div class="row" id="login_setup_div" >
      <div class="content-left" id="login_tip">
        <img src="/luci-static/resources/image/login/login-tip.png" width="470" height="283"
alt=""/>
      </div>
      <div class="content-right content-offset">
         <br/>
        <br/>
        <font face="微软雅黑" style="font-size: 20px;">用户登录</font>
        <font face="Arial" style="font-size: 14px;"> LOGIN</font>
        <form id="login_form" method="post" action="/cgi-bin/luci" onsubmit="return
checkPassword();">
          <div class="login-input">
          <div class="login-block" style="background:white url(/luci-
static/resources/image/login/login_user-1.png) no-repeat left;">
          <input type="text" placeholder="Username" class="form-control" id="login_username"
name="username" value="useradmin">

...
...
...
```

参 发现可能的服务器路径泄露模式 1

TOC

问题 1 / 1

TOC

发现可能的服务器路径泄露模式

严重性:	参考
CVSS 分数:	0.0
URL:	http://192.168.1.1:8080/js/jquery.js
实体:	jquery.js (Page)
风险:	可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息
原因:	未安装第三方产品的最新补丁或最新修补程序
固定值:	为 Web 服务器或 Web 应用程序下载相关的安全补丁

差异:

推理: 响应包含服务器上文件的绝对路径和/或文件名。

测试请求和响应:

```
GET /js/jquery.js?v=20250327153146 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1:8080/maintain
Connection: keep-alive
Host: 192.168.1.1:8080
Accept: */*
Accept-Language: en-US


HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 285313
Cache-control: public,max-age=86400
Content-Type: application/x-javascript

/*!
 * jQuery JavaScript Library v3.7.1
 * https://jquery.com/
 *
 * Copyright OpenJS Foundation and other contributors
 * Released under the MIT license
 * https://jquery.org/license
 *
 * Date: 2023-08-28T13:37Z
 */
( function( global, factory ) {

 "use strict";

 if ( typeof module === "object" && typeof module.exports === "object" ) {

         // For CommonJS and CommonJS-like environments where a proper `window`
         // is present, execute the factory and get jQuery.
         // For environments that do not have a `window` with a `document`
         // (such as Node.js), expose a factory as module.exports.
         // This accentuates the need for the creation of a real `window`.
         // e.g. var jQuery = require("jquery")(window);
         // See ticket trac-14549 for more info.
         module.exports = global.document ?
                 factory( global, true ) :
                 function( w ) {
                         if ( !w.document ) {
                                 throw new Error( "jQuery requires a window with a
document" );
                                }
                         return factory( w );
                 }       ;
 } else {
         factory( global );
        }

// Pass this if window is not defined yet
} )( typeof window !== "undefined" ? window : this, function( window, noGlobal ) {

// Edge <= 12 - 13+, Firefox <=18 - 45+, IE 10 - 11, Safari 5.1 - 9+, iOS 6 - 9.1
// throw exceptions when non-strict code (e.g., ASP.NET 4.5) accesses strict mode
// arguments.callee.caller (trac-13335). But as of jQuery 3.0 (2016), strict mode should be
common
// enough that all such attempts are guarded in a try block.
"use strict";

var arr = [];

var getProto = Object.getPrototypeOf;

var slice = arr.slice;

var flat = arr.flat ? function( array ) {
 return arr.flat.call( array );
} : function( array ) {
 return arr.concat.apply( [], array );
};


var push = arr.push;
```

```
var indexOf = arr.indexOf;

var class2type = {};

var toString = class2type.toString;

var hasOwn = class2type.hasOwnProperty;

var fnToString = hasOwn.toString;

var ObjectFunctionString = fnToString.call( Object );

var support = {};

var isFunction = function isFunction( obj ) {

         // Support: Chrome <=57, Firefox <=52
         // In some browsers, typeof returns "function" for HTML <object> elements
         // (i.e., `typeof document.createElement( "object" ) === "function"`).
         // We don't want to classify *any* DOM node as a function.
         // Support: QtWeb <=3.8.5, WebKit <=534.34, wkhtmltopdf tool <=0.12.5
         // Plus for old WebKit, typeof returns "function" for HTML collections
         // (e.g., `typeof document.getElementsByTagName("div") === "function"`). (gh-
4756)
         return typeof obj === "function" && typeof obj.nodeType !== "number" &&
                 typeof obj.item !== "function";
 };


var isWindow = function isWindow( obj ) {
         return obj != null && obj === obj.window;
 };


var document = window.document;



 var preservedScriptAttributes = {
         type: true,
         src: true,
         nonce: true,
         noModule: true
 };

 function DOMEval( code, node, doc ) {
         doc = doc || document;

         var i, val,
                 script = doc.createElement( "script" );

         script.text = code;
         if ( node ) {
                 for ( i in preservedScriptAttributes ) {

                         // Support: Firefox 64+, Edge 18+
                         // Some browsers don't support the "nonce" property on scripts.
                         // On the other hand, just using `getAttribute` is not enough as
                         // the `nonce` attribute is reset to an empty string whenever it
                         // becomes browsing-context connected.
                         // See https://github.com/whatwg/html/issues/2369
                         // See https://html.spec.whatwg.org/#nonce-attributes
                         // The `node.getAttribute` check was added for the sake of
                         // `jQuery.globalEval` so that it can fake a nonce-containing
node
                         // via an object.
                         val = node[ i ] || node.getAttribute && node.getAttribute( i );
                         if ( val ) {
                                 script.setAttribute( i, val );
                                }
                        }
                }
         doc.head.appendChild( script ).parentNode.removeChild( script );
        }


function toType( obj ) {
```

```
 if ( obj == null ) {
         return obj + "";
        }

 // Support: Android <=2.3 only (functionish RegExp)
 return typeof obj === "object" || typeof obj === "function" ?
         class2type[ toString.call( obj ) ] || "object" :
         typeof obj;
}
/* global Symbol */
// Defining this global in .eslintrc.json would create a danger of using the global
// unguarded in another place, it seems safer to define global only for this module


var version = "3.7.1",

 rhtmlSuffix = /HTML$/i,

 // Defi
...
...
...

var whitespace = "[\\x20\\t\\r\\n\\f]";
...
...
...
 // https://www.w3.org/TR/css-syntax-3/#ident-token-diagram
 identifier = "(?:\\\\[\\da-fA-F]{1,6}" + whitespace +
         "?|\\\\[^\\r\\n\\f]|[\\w-]|[^\0        -\\x7f])+",
...
...
...
```

参 发现内部 IP 泄露模式 1 TOC

问题 1 / 1 TOC

发现内部 IP 泄露模式

严重性:	参考
CVSS 分数:	0.0
URL:	http://192.168.1.1:8080/login.html
实体:	login.html (Page)
风险:	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因:	Web 应用程序编程或配置不安全
固定值:	除去 Web 站点中的内部 IP 地址

差异:

推理: AppScan 在响应中发现了看似为内部 IP 地址的内容。

测试请求和响应:

```
GET /login.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1:8080/
Connection: keep-alive
Host: 192.168.1.1:8080
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 8226
Content-Type: text/html

<!DOCTYPE html>
<html lang="en">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge">
 <meta name="viewport" content="width=device-width, initial-scale=1">
 <meta HTTP-EQUIV='Pragma' CONTENT='no-cache'>
 <title>       中国电信智能网关</title>
 <link href="/css/login.css?v=20250327153146" rel="stylesheet">
 <link href="/css/main_style.css?v=20250327153146" rel="stylesheet">
 <script src="/js/jquery.js?v=20250327153146"></script>
 <script src="/js/aes_1.js?v=20250327153146"></script>
 <script src="/js/common.js?v=20250327153146"></script>
  <script>
         var g_wlan24_num=8
         var g_wlan58_num=8
         var g_usb_num=1
         var g_province="JT"
  </script>
</head>
<body>
 <script>
 var is_80_login = false
 var login_err = getQueryVariable("login_err")
 var username = getQueryVariable("username")
 var psd = getQueryVariable("psd")

 $(document).ready(function(){

         /       /海南电信需求：新增路由设置功能
         if (g_province == "HAI") {
                 $("#route_set_span").show()
                 $.ajax({
                         url: '/boaform/global_attr_get.cgi',
                         type: 'post',
                         success: function(rsp, status, xhr){
                                 var data = JSON.parse(rsp).data
                                 if (data.ulRouteStatus == "0") {
                                         $("#route_set_span input").attr("disabled",
false)
                                 }
                         }       ,
                 }       )
                }

         /       /非集团版本，显示注册按钮。注册成功后禁用注册按钮
         if (g_province != "JT") {
                 $("#register_span").show()
                 $.ajax({
                         url: '/boaform/web_Capability_show.cgi',
                         type: 'post',
                         success: function(rsp, status, xhr){
                                 var data = JSON.parse(rsp).data
                                 if (!(data.g_status == "0" && data.g_result == "1")) {
                                         $("#register_span input").attr("disabled", false)
                                 }
                         }       ,
                 }       )
                }
```

```
        if (login_err) {
                is_80_login = true
                login_err_info(login_err)
        } else {
                if (username && psd) {
                        psd = decodeURI(psd)
                        is_80_login = true
                        login()
                       }
               }
})

function login_hint(msg)
       {
        pop_window.alert({
                                title:"       登入提示",
                                text:msg,
                                confirm:true,
                                close:function(){
                                        if (is_80_login)
                                                window.location = location.protocol +
"//" + location.hostname;
                                }       ,
                        }       )
       }

function login_err_info(err) {
        if (err == "success_telecomadmin") {
                window.location = "/admin/status_overview_ip.html";
        } else if (err == "success_useradmin") {
                login_hint("       账号或密码错误，请重新登录！")
        } else if(err == "invalid_username") {
                login_hint("       账号或密码错误，请重新登录！")
        } else if(err == "bad_password"){
                login_hint("       账号或密码错误，请重新登录！")
        } else if(err == "invalid_password"){
                login_hint("       账号或密码错误，请重新登录！")
        } else if(err == "three_error_login") {
                login_hint("       密码错误三次，请一分钟之后重新登录！")
        } else if (err == "one_user_login") {
                login_hint("       当前已有一个用户已登陆，退出已登陆用户重试！");
        } else if (err == "telecomadmin_disabled_err") {
                login_hint("       维护账号使能未打开！");
        } else {
                login_hint("       未知的错误");
               }
       }

function createXmlhttp () {
        if (window.XMLHttpRequest) {
                /       /针对FireFox，Mozillar，Opera，Safari，IE7，IE8
                xmlhttp = new XMLHttpRequest();
                /       /针对某些特定版本的mozillar浏览器的BUG进行修正
                if (xmlhttp.overrideMimeType) {
                          xmlhttp.overrideMimeType("text/xml");
                   }
        }else if (window.ActiveXObject) {
                /       /针对IE6，IE5.5，IE5
                /       /两个可以用于创建XMLHTTPRequest对象的控件名称，保存在一个js的数组中
                /       /排在前面的版本较新
                var activexName = ["MSXML2.XMLHTTP","Microsoft.XMLHTTP"];
                for (var i = 0; i < activexName.length; i++) {
                        try       {
                                /       /取出一个控件名进行创建，如果创建成功就终止循环
                                /       /如果创建失败，回抛出异常，然后可以继续循环，继续尝试创建
                                xmlhttp = new ActiveXObject(activexName[i]);
                                break;
                        } catch(e){
                               }
                       }
               }
       }

function sendRequest(url,param,callback){
        createXmlhttp ();
        try{
                //xmlhttp.onreadystatechange = processResponse;  //       回调方法
                xmlhttp.open("post",url ,false); // true       异步
```

```
                xmlhttp.setRequestHeader("content-type","application/x-www-form-
urlencoded");
                xmlhttp.setRequestHeader("Cache-Control", "no-cache");
                var str = ''
                for(var i in param){
                        str += i + "=" + encodeURIComponent(param[i]) + "&";
                       }
                str = str.substring(0,str.length -1);
                xmlhttp.send(str);

                var str = xmlhttp.responseText;
                var webdata = eval("("+str+")");
                if (webdata){
                        webdata = webdata.data;
                       }
                if(callback)
                        {
                        callback(webdata);
                       }

         }catch(e){
                }
        }

 function route_set() {
         window.location = "/route_set.html"
        }

 function login() {
                var data
                if (is_80_login) {
                        data = {
                                web_login_name: username,
                                web_login_password: psd,
                               }
                } else {
                        data = {
                                        w
...
...
...

         $("#login_password").val("")
        }

 function register() {
         window.location = "http://       192.168.1.1:8080/register.html"
        }
 </script>
 <div class="wraplogin">
         <div id="top" style="width:100%;"></div>
...
...
...
```

修订建议

中 安装 WebLogic 的最新版本和补丁 TOC

该任务修复的问题类型

- BEA WebLogic URL 欺骗目录列表

常规

升级至供应商站点所提供的 Weblogic 最新版本。请务必使用所有可用的及最近的补丁。使用专为了解决这个问题而确定的补丁，并不能保护服务器免于其他攻击。

低 除去 HTML 注释中的敏感信息 TOC

该任务修复的问题类型

- HTML 注释敏感信息泄露

常规

[1] 请勿在 HTML 注释中遗留任何重要信息（如文件名或文件路径）。
[2] 从生产站点注释中除去以前（或未来）站点链接的跟踪信息。
[3] 避免在 HTML 注释中放置敏感信息。
[4] 确保 HTML 注释不包括源代码片段。
[5] 确保程序员没有遗留重要信息。

低 除去 Web 站点中的内部 IP 地址 TOC

该任务修复的问题类型

- 发现内部 IP 泄露模式

常规

内部 IP 通常显现在 Web 应用程序/服务器所生成的错误消息中，或显现在 HTML/JavaScript 注释中。
[1] 关闭 Web 应用程序/服务器中有问题的详细错误消息。
[2] 确保已安装相关的补丁。
[3] 确保内部 IP 信息未留在 HTML/JavaScript 注释中。

低 将服务器配置为使用安全策略的“Content-Security-Policy”头 TOC

该任务修复的问题类型

- “Content-Security-Policy”头缺失或不安全

常规

将服务器配置为发送“Content-Security-Policy”头。
关于 Apache，请参阅：
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
关于 IIS，请参阅：
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
关于 nginx，请参阅：
http://nginx.org/en/docs/http/ngx_http_headers_module.html

低 将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头 TOC

该任务修复的问题类型

- “X-XSS-Protection”头缺失或不安全

常规

配置您的服务器，以确保在所有传出请求上发送值为“1”（即已启用）的“X-XSS-Protection”报头。

关于 Apache，请参阅：
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
关于 IIS，请参阅：
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
关于 nginx，请参阅：
http://nginx.org/en/docs/http/ngx_http_headers_module.html

低 将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头 TOC

该任务修复的问题类型

- “X-Content-Type-Options”头缺失或不安全

常规

将服务器配置为针对所有外发请求发送具有值“nosniff”的“X-Content-Type-Options”头。

关于 Apache，请参阅：
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
关于 IIS，请参阅：
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
关于 nginx，请参阅：
http://nginx.org/en/docs/http/ngx_http_headers_module.html

低 请勿接受在查询字符串中发送的主体参数 TOC

该任务修复的问题类型

- 查询中接受的主体参数

常规

重新对应用程序编程以禁用对查询中列出的 POST 参数的处理

低 为 Web 服务器或 Web 应用程序下载相关的安全补丁 TOC

该任务修复的问题类型

- 发现可能的服务器路径泄露模式

常规

有几种缓解技术：
[1] 如果漏洞存在于应用程序内，请修复服务器代码，以使得任何输出中都不包含文件位置。
[2] 否则，如果应用程序位于第三方产品中，请根据 Web 服务器或 Web 应用程序上使用的第三方产品下载相关的安全补丁。

咨询

BEA WebLogic URL 欺骗目录列表

TOC

测试类型：
基础结构测试

威胁分类：
目录索引

原因：
未安装第三方产品的最新补丁或最新修订程序

安全性风险：
可能会查看和下载特定 Web 应用程序虚拟目录的内容，其中可能包含受限文件

受影响产品：

CWE:
548

X-Force：
5588

引用：
供应商站点

技术描述：
***
请注意，如果其他目录列表在相同资源上测试成功，那么该问题可能表现为“非漏洞”。
***

在所要的目录路径上附加特定 URL 编码字符（也就是 NULL、/、\ 和点），便可能略过对于目录浏览的保护。利用的样本：
GET /PATH/ESCAPE_CHAR/ HTTP/1.0

其中 PATH 是要查看的路径，ESCAPE_CHAR 是 %00、%2F、%5C、%2E 的其中之一。

“Content-Security-Policy”头缺失或不安全

TOC

测试类型：

应用程序级别测试

威胁分类：

信息泄露

原因：

Web 应用程序编程或配置不安全

安全性风险：

- 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
-

受影响产品：

CWE:

200

引用：

有用 HTTP 头列表
内容安全策略简介
MDN Web 文档 - 内容安全策略

技术描述：

“内容安全策略”标头旨在修改浏览器呈现页面的方式，从而防止各种跨站点注入，包括跨站点脚本。以不妨碍网站正常运行的方式正确设置标头值非常重要。例如，如果将标头设置为阻止执行内联 JavaScript，则网站不得在其页面中使用内联 JavaScript。
为了防止跨站点脚本、跨框架脚本和点击劫持，使用适当的值设置以下策略非常重要：
'default-src' 和 'frame-ancestors'策略、*或*所有 'script-src'、'object-src' 和 'frame-ancestors' 策略。
对于 'default-src'、'script-src' 和 'object-src'，应避免使用不安全的值，例如 '*'、'data:'、'unsafe-inline' 或 'unsafe-eval'。
对于 'frame-ancestors'，应避免使用不安全的值，例如 '*' 或 'data:'。
有关更多信息，请参阅以下链接。

“X-Content-Type-Options”头缺失或不安全

TOC

测试类型：

应用程序级别测试

威胁分类：
信息泄露

原因：
Web 应用程序编程或配置不安全

安全性风险：
- 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
-

受影响产品：

CWE:
200

引用：
有用 HTTP 头列表
减少 MIME 类型安全风险

技术描述：
“X-Content-Type-Options”头（具有“nosniff”值）防止 IE 和 Chrome 忽略响应的内容类型。
此操作可能防止不可信内容（例如，用户上载内容）在用户浏览器上执行（例如，在恶意命名之后）。

“X-XSS-Protection”报头缺失或不安全

TOC

测试类型：
应用程序级别测试

威胁分类：
信息泄露

原因：
Web 应用程序编程或配置不安全

安全性风险：
- 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
-

受影响产品：

CWE:

200

引用：

有用 HTTP 头列表
IE XSS 过滤器

技术描述：

值为‘1’的“X-XSS-Protection”报头强制跨站点脚本编制过滤器进入启用模式，即使用户已禁用。
此过滤器内置于最新版本的 Web 浏览器（IE 8 +、Chrome 4+）中，在缺省情况下通常为已启用状态。虽然此过滤器不是第一个也不是唯一一个针对跨站点脚本编制的防御程序，但它可以作为额外保护层。

查询中接受的主体参数

TOC

测试类型：

应用程序级别测试

威胁分类：

信息泄露

原因：

Web 应用程序编程或配置不安全

安全性风险：

- 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
- 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息

受影响产品：

CWE:

200

引用：

超文本传输协议 (HTTP/1.1) 语义和内容：
GET
POST

技术描述：

GET 请求设计的目的在于查询服务器，而 POST 请求用于提交数据。但是，除了技术目的之外，攻击查询参数比攻击主体参数更容易，因为向原始站点发送链接或在博客或注释中发布链接更容易，而且得到的结果比另一种方法更好，为了攻击带有主体参数的请求，攻击者需要创建其中包含表单的页面，当受害者访问表单时就会提交表单。
说服受害者访问他不了解的页面比让受害者访问原始站点要难很多。因此，不建议支持可到达查询字符串的主体参数。

HTML 注释敏感信息泄露

TOC

测试类型：
应用程序级别测试

威胁分类：
信息泄露

原因：
程序员在 Web 页面上留下调试信息

安全性风险：
可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置

受影响产品：

CWE:
615

X-Force：
52601

引用：
WASC 威胁分类：信息泄露

技术描述：
很多 Web 应用程序程序员使用 HTML 注释，以在需要时帮助调试应用程序。尽管添加常规注释有助于调试应用程序，但一些程序员往往会遗留重要数据（例如：与 Web 应用程序相关的文件名、旧的链接或原非供用户浏览的链接、旧的代码片段等）。

发现可能的服务器路径泄露模式

TOC

测试类型：
应用程序级别测试

威胁分类：
信息泄露

原因：
未安装第三方产品的最新补丁或最新修补程序

安全性风险：
可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息

受影响产品：

CWE:
200

X-Force：
52839

技术描述：
AppScan 检测到包含文件绝对路径的响应（例如，Windows 中的 c:\dir\file，或 Unix 中的 /dir/file）。

攻击者可能能够利用这一信息访问服务器机器目录结构上的敏感信息，进而对站点发起进一步攻击。

发现内部 IP 泄露模式

TOC

测试类型：
应用程序级别测试

威胁分类：
信息泄露

原因：
Web 应用程序编程或配置不安全

安全性风险：
可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置

受影响产品：

CWE:
200

X-Force：
52657

技术描述：

AppScan 检测到包含内部 IP 地址的响应。
内部 IP 定义为以下 IP 范围内的 IP：
10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255

内部 IP 公开对于攻击者非常有价值，因为它揭示了内部网络的 IP 联网模式。获知内部网络的 IP 联网模式可能会帮助攻击者计划针对内部网络的进一步攻击。

应用程序数据

已访问的 URL 13

TOC

URL
http://192.168.1.1/
http://192.168.1.1/cgi-bin/luci
http://192.168.1.1/luci-static/resources/js/util.js?version=5200
http://192.168.1.1/luci-static/resources/js/jquery.js?version=5200
http://192.168.1.1/luci-static/resources/js/login.js?version=5200
http://192.168.1.1/cgi-bin/luci
http://192.168.1.1:8080/maintain
http://192.168.1.1:8080/js/aes_1.js?v=20250327153146
http://192.168.1.1:8080/js/jquery.js?v=20250327153146
http://192.168.1.1:8080/js/common.js?v=20250327153146
http://192.168.1.1:8080/login.html
http://192.168.1.1:8080/boaform/passwd_key_show.cgi
http://192.168.1.1:8080/boaform/web_login_exe.cgi

参数 10

TOC

名称	值	URL	类型
web_login_password	eda7688a7f9fdb14bd1e592df15fe5879bb8439cf139555eb174a47639ac085b	http://192.168.1.1:8080/boaform/web_login_exe.cgi	密码
version	5200	http://192.168.1.1/luci-static/resources/js/login.js?version=5200	简单链接
v	20250327153146	http://192.168.1.1:8080/js/aes_1.js?v=20250327153146	简单链接
psd		http://192.168.1.1/cgi-bin/luci	隐藏
version	5200	http://192.168.1.1/luci-static/resources/js/util.js?version=5200	简单链接
version	5200	http://192.168.1.1/luci-static/resources/js/jquery.js?version=5200	简单链接
username	telecomadmin	http://192.168.1.1/cgi-bin/luci	隐藏

v	20250327153146	http://192.168.1.1:8080/js/common.js?v=20250327153146	简单链接
web_login_name		http://192.168.1.1:8080/boaform/web_login_exe.cgi	文本
v	20250327153146	http://192.168.1.1:8080/js/jquery.js?v=20250327153146	简单链接

失败的请求 6

TOC

URL	原因
http://192.168.1.1/luci-static/resources/?version=5200	响应状态“400” — 错误请求
http://192.168.1.1/luci-static/resources/js/?version=5200	响应状态“400” — 错误请求
http://192.168.1.1/luci-static/?version=5200	响应状态“400” — 错误请求
http://192.168.1.1/luci-static/resources/image/	响应状态“400” — 错误请求
http://192.168.1.1/luci-static/resources/css/?version=5200	响应状态“400” — 错误请求
http://192.168.1.1/luci-static/resources/image/login/	响应状态“400” — 错误请求

已过滤的 URL 10

TOC

URL	原因
http://192.168.1.1/luci-static/resources/image/favicon.ico	文件扩展名
http://192.168.1.1/luci-static/resources/css/login.css?version=5200	文件扩展名
http://192.168.1.1/luci-static/resources/image/logo_tianyi.png	文件扩展名
http://192.168.1.1/luci-static/resources/image/line.png	文件扩展名
http://192.168.1.1/luci-static/resources/image/login/login-tip.png	文件扩展名
http://192.168.1.1:8080/css/login.css?v=20250327153146	文件扩展名
http://192.168.1.1:8080/css/main_style.css?v=20250327153146	文件扩展名
http://192.168.1.1:8080/image/loading.gif	文件扩展名
http://192.168.1.1:8080/	类似 DOM
http://192.168.1.1/cgi-bin/luci	类似 DOM

注释 2

TOC

URL	注释
http://192.168.1.1/	<!DOCTYPE html>
http://192.168.1.1/cgi-bin/luci	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

JavaScript 19

TOC

URL / 代码

http://192.168.1.1/luci-static/resources/js/util.js

```
var WEB_POLL_INTERVAL=5;

window.console = window.console || (function(){
    var c = {}; c.log = c.warn = c.debug = c.info = c.error = c.time = c.dir = c.profile
    = c.clear = c.exception = c.trace = c.assert = function(){};
    return c;
})();

var noWiFi = (window.localStorage.getItem("hasWiFi") == 1) ? 0 : 1;
var noPots = (window.localStorage.getItem("hasPots") == 1) ? 0 : 1;
var noUsb = (window.localStorage.getItem("hasUsb") == 1) ? 0 : 1;
var noMesh = (window.localStorage.getItem("hasMesh") == 1) ? 0 : 1;
var devType = window.localStorage.getItem("devType");

function isIE7Browser()
{
 if(navigator.appName == "Microsoft Internet Explorer" && navigator.appVersion.match(/7./i)=="7.")
 {
         return true;
        }
 else
        {
         return false;
        }
}
function judedNavation()
{
 if(navigator.appName == "Microsoft Internet Explorer" && navigator.appVersion.match(/6./i)=="6."){
         return 6;
 }
 else if(navigator.appName == "Microsoft Internet Explorer" &&
navigator.appVersion.match(/7./i)=="7."){
         return 7;
 }
 else if(navigator.appName == "Microsoft Internet Explorer" &&
navigator.appVersion.match(/8./i)=="8."){
         return 8;
 }
 else if(navigator.appName == "Microsoft Internet Explorer" &&
navigator.appVersion.match(/9./i)=="9."){
         return 9;
        }
 else{
         return 10;
        }
}


function createInput(id, name, placeholder, maxlength, type, value)
{
 var inputObj = "<input ";
 if ( id != "" && id != "undefined" )
        {
         inputObj += "id='" + id + "' ";
        }
 if ( name != "" && name != "undefined" )
        {
         inputObj += "name='" + name + "' ";
        }
 if ( placeholder != "" && placeholder != "undefined" )
        {
         inputObj += "placeholder='" + placeholder + "' ";
```

```
        }
 if ( maxlength != "" && maxlength != "undefined" )
        {
         inputObj += "maxlength='" + maxlength + "' ";
        }
 inputObj += "type='" + type + "' ";
 inputObj += "value='" + value + "' ";
 inputObj += ">";
 return inputObj;
}

function inputBindFocus()
{
 $("input[type='password'], .password_content input[type='text']").bind("focusin", function(){
         $(this).parent().eq(0).addClass("password_content_focus");
         if ( !$(this).next().hasClass("password_switch_eyeon") )
                {
         $(this).next().addClass("password_switch_focus");
                }
 });
 $("input[type='password'], .password_content input[type='text']").bind("focusout", function(){
         $(this).parent().eq(0).removeClass("password_content_focus");
         $(this).next().removeClass("password_switch_focus");
 });
}

function customSwitchInit()
{
 $(".switch_content").bind("click", function(){
         if($(this).hasClass("switch_content_on")){
                 $(this).removeClass("switch_content_on");
                 $(this).addClass("switch_content_off");
                 $(this).children("span").html("OFF ");
                 $("#" + $(this).attr("id") + "_value").val(0);
         }else{
                 $(this).addClass("switch_content_on");
                 $(this).removeClass("switch_content_off");
                 $(this).children("span").html(" ON");
                 $("#" + $(this).attr("id") + "_value").val(1);
                }
         console.log($("#" + $(this).attr("id") + "_value").val());
 });
}
function customSelectInit()
{
 $(".select-arrow").click(function(){
         $(this).parent().addClass("select-open");
         });

 //Èç¹ûÊó±êÎòÏÂ»¬¶¯£¬Ôò²»ÒþÂØ
 $(".dropdown-select").bind("mouseleave",
                 function(e)
                 {
                         var w = $(this).width();
                         var h = $(this).height();
                         var x = (e.pageX - this.offsetLeft - (w / 2)) * (w > h ? (h / w) : 1);
                         var y = (e.pageY - this.offsetTop - (h / 2)) * (h > w ? (w / h) : 1);
                         var direction = Math.round((((Math.atan2(y, x) * (180 / Math.PI)) + 180) /
90) + 3) % 4;
                         if(direction != 2)
                         {
                                 $(this).removeClass("select-open");
                                }
 });

 $(".dropdown-menu-select").mouseleave(function(){
         $(this).parent().removeClass("select-open");
 });

 $(".dropdown-menu-select li").click(function(){
         $(this).parent().siblings("label").first().text($(this).text());
         $("#" + $(this).parent().attr("id") + "_value").val($(this).attr("livalue"));
         $(this).parent().parent().removeClass("select-open");;
 });
}
function customPasswordInit()
{
 inputBindFocus();
```

```
 $(".password_switch").bind("click", function(){
        if( $(this).css("background-image").indexOf("eye_close") > -1 )
               {
                $(this).removeClass("password_switch_unfocus");
                $(this).removeClass("password_switch_focus");
                $(this).addClass("password_switch_eyeon");
               }
        else
               {
                $(this).removeClass("password_switch_eyeon");
                $(this).addClass("password_switch_unfocus");
               }

        if( 9 > judedNavation() )
               {
                var $pwdInput = $(this).parent(".password_content").find("input");
                if($pwdInput.attr("type").indexOf("password") != -1){
                        var inputStr = createInput($pwdInput.attr("id"), $pwdInput.attr("name"),
$pwdInput.attr("placeholder"), $pwdInput.attr("maxlength"), "text", $pwdInput.val());
                        $pwdInput.replaceWith($(inputStr));
                 }else{
                        var inputStr = createInput($pwdInput.attr("id"), $pwdInput.attr("name"),
$pwdInput.attr("placeholder"), $pwdInput.attr("maxlength"), "password", $pwdInput.val());
                        $pwdInput.replaceWith($(inputStr));
                       }
               }
        els...
```

http://192.168.1.1/luci-static/resources/js/jquery.js

```
/*! jQuery v3.3.1 | (c) JS Foundation and other contributors | jquery.org/license */
!function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports?
module.exports=e.document?t(e,!0):function(e){if(!e.document)throw new Error("jQuery requires a window with a
document");return t(e)}:t(e)}("undefined"!=typeof window?window:this,function(e,t){"use strict";var n=
[],r=e.document,i=Object.getPrototypeOf,o=n.slice,a=n.concat,s=n.push,u=n.indexOf,l=
{},c=l.toString,f=l.hasOwnProperty,p=f.toString,d=p.call(Object),h={},g=function e(t)
{return"function"==typeof t&&"number"!=typeof t.nodeType},y=function e(t){return null!=t&&t===t.window},v=
{type:!0,src:!0,noModule:!0};function m(e,t,n){var i,o=(t=t||r).createElement("script");if(o.text=e,n)for(i
in v)n[i]&&(o[i]=n[i]);t.head.appendChild(o).parentNode.removeChild(o)}function x(e){return null==e?
e+"":"object"==typeof e||"function"==typeof e?l[c.call(e)]||"object":typeof e}var b="3.3.1",w=function(e,t)
{return new w.fn.init(e,t)},T=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g;w.fn=w.prototype=
{jquery:"3.3.1",constructor:w,length:0,toArray:function(){return o.call(this)},get:function(e){return
null==e?o.call(this):e<0?this[e+this.length]:this[e]},pushStack:function(e){var
t=w.merge(this.constructor(),e);return t.prevObject=this,t},each:function(e){return
w.each(this,e)},map:function(e){return this.pushStack(w.map(this,function(t,n){return
e.call(t,n,t)}))},slice:function(){return this.pushStack(o.apply(this,arguments))},first:function(){return
this.eq(0)},last:function(){return this.eq(-1)},eq:function(e){var t=this.length,n=+e+(e<0?t:0);return
this.pushStack(n>=0&&n<t?[this[n]]:[])},end:function(){return
this.prevObject||this.constructor()},push:s,sort:n.sort,splice:n.splice},w.extend=w.fn.extend=function(){var
e,t,n,r,i,o,a=arguments[0]||{},s=1,u=arguments.length,l=!1;for("boolean"==typeof a&&(l=a,a=arguments[s]||
{},s++),"object"==typeof a||g(a)||(a={}),s===u&&(a=this,s--);s<u;s++)if(null!=(e=arguments[s]))for(t in
e)n=a[t],a!==(r=e[t])&&(l&&r&&(w.isPlainObject(r)||(i=Array.isArray(r)))?(i?(i=!1,o=n&&Array.isArray(n)?n:
[]):o=n&&w.isPlainObject(n)?n:{},a[t]=w.extend(l,o,r)):void 0!==r&&(a[t]=r));return
a},w.extend({expando:"jQuery"+("3.3.1"+Math.random()).replace(/\D/g,""),isReady:!0,error:function(e){throw
new Error(e)},noop:function(){},isPlainObject:function(e){var t,n;return!(!e||"[object
Object]"!==c.call(e))&&(!
(t=i(e))||"function"==typeof(n=f.call(t,"constructor")&&t.constructor)&&p.call(n)===d)},isEmptyObject:functio
n(e){var t;for(t in e)return!1;return!0},globalEval:function(e){m(e)},each:function(e,t){var n,r=0;if(C(e))
{for(n=e.length;r<n;r++)if(!1===t.call(e[r],r,e[r]))break}else for(r in
e)if(!1===t.call(e[r],r,e[r]))break;return e},trim:function(e){return null==e?"":
(e+"").replace(T,"")},makeArray:function(e,t){var n=t||[];return null!=e&&(C(Object(e))?
w.merge(n,"string"==typeof e?[e]:e):s.call(n,e)),n},inArray:function(e,t,n){return null==t?-
1:u.call(t,e,n)},merge:function(e,t){for(var n=+t.length,r=0,i=e.length;r<n;r++)e[i++]=t[r];return
e.length=i,e},grep:function(e,t,n){for(var r,i=[],o=0,a=e.length,s=!n;o<a;o++)
(r=!t(e[o],o))!==s&&i.push(e[o]);return i},map:function(e,t,n){var r,i,o=0,s=
[];if(C(e))for(r=e.length;o<r;o++)null!=(i=t(e[o],o,n))&&s.push(i);else for(o in e)null!=
(i=t(e[o],o,n))&&s.push(i);return a.apply([],s)},guid:1,support:h}),"function"==typeof Symbol&&
(w.fn[Symbol.iterator]=n[Symbol.iterator]),w.each("Boolean Number String Function Array Date RegExp Object
Error Symbol".split(" "),function(e,t){l["[object "+t+"]"]=t.toLowerCase()});function C(e){var
t=!!e&&"length"in e&&e.length,n=x(e);return!g(e)&&!y(e)&&("array"===n||0===t||"number"==typeof t&&t>0&&t-1 in
e)}var E=function(e){var t,n,r,i,o,a,s,u,l,c,f,p,d,h,g,y,v,m,x,b="sizzle"+1*new
Date,w=e.document,T=0,C=0,E=ae(),k=ae(),S=ae(),D=function(e,t){return e===t&&(f=!0),0},N={}.hasOwnProperty,A=
[],j=A.pop,q=A.push,L=A.push,H=A.slice,O=function(e,t){for(var n=0,r=e.length;n<r;n++)if(e[n]===t)return
```

```
n;return-
1},P="checked|selected|async|autofocus|autoplay|controls|defer|disabled|hidden|ismap|loop|multiple|open|reado
nly|required|scoped",M="[\\x20\\t\\r\\n\\f]",R="(?:\\\\.|[\\w-]|[^\0-\\xa0])+",I="\\["+M+"*("+R+")(?:"+M+"*
([*^$|!~]?=)"+M+"*(?:'((?:\\\\.|[^\\\\'])*)'|\"((?:\\\\.|[^\\\\\"])*)\"|("+R+"))|)"+M+"*\\]",W=":("+R+")(?:\\
(('((?:\\\\.|[^\\\\'])*)'|\"((?:\\\\.|[^\\\\\"])*)\")|((?:\\\\.|[^\\\\()[\\]]|"+I+")*)|.*)\\)|)",$=new
RegExp(M+"+","g"),B=new RegExp("^"+M+"+|((?:^|[^\\\\])(?:\\\\.)*)"+M+"+$","g"),F=new
RegExp("^"+M+"*,"+M+"*"),_=new RegExp("^"+M+"*([>+~]|"+M+")"+M+"*"),z=new RegExp("="+M+"*
([^\\]'\"]*?)"+M+"*\\]","g"),X=new RegExp(W),U=new RegExp("^"+R+"$"),V={ID:new RegExp("^#("+R+")"),CLASS:new
RegExp("^\\.("+R+")"),TAG:new RegExp("^("+R+"|[*])"),ATTR:new RegExp("^"+I),PSEUDO:new
RegExp("^"+W),CHILD:new RegExp("^:(only|first|last|nth|nth-last)-(child|of-type)(?:\\("+M+"*(even|odd|(([+-
]|)(\\d*)n|)"+M+"*(?:([+-]|)"+M+"*(\\d+)|))"+M+"*\\)|)","i"),bool:new RegExp("^(?:"+P...
```

http://192.168.1.1/cgi-bin/luci

```
window.onload =function() {console.log("The device support WiFi: " + 1);console.log("The device support USB:
" + 1);console.log("The device type: " + 9);window.localStorage.setItem("hasWiFi",
1);window.localStorage.setItem("hasPots", 1);window.localStorage.setItem("hasUsb",
1);window.localStorage.setItem("hasMesh", 1);window.localStorage.setItem("devType", 9);}    function
hideHint()  {  $(".login-input").children(":last").remove();
$("#login_username").removeAttr("disabled");$("#login_password").removeAttr("disabled");  }
```

http://192.168.1.1/cgi-bin/luci

```
    if (bType == "IE8")    {var speed=6;console.log("Current broswer is IE8.");    function Marquee(){
if(document.getElementById("line2").offsetWidth-document.getElementById("line").scrollLeft<=0)
document.getElementById("line").scrollLeft-=document.getElementById("line1").offsetWidth;      else{
document.getElementById("line").scrollLeft++;      }    }   setInterval(Marquee,speed);   }
```

http://192.168.1.1/cgi-bin/luci

```
function isIPv6Addr(str){        return /:/.test(str) &&          str.match(/:/g).length<8 &&
/::/.test(str)          ?(str.match(/::/g).length==1 &&          /^::$|^(::)?([\da-f]{1,4}(:|::))*[\da-f]
{1,4}(:|::)?$/i.test(str))          :/^([\da-f]{1,4}:){7}[\da-f]{1,4}$/i.test(str);}if
(isIPv6Addr(location.host))var hosturl = "[" + location.host + "]";elsevar hosturl = location.host;
document.write("<a href='" + location.protocol + "//" + hosturl + ":8080/maintain" + "'>快速装维入口</a>");
```

http://192.168.1.1/cgi-bin/luci

```
keyCapscheck(event, 1)
```

http://192.168.1.1/cgi-bin/luci

```
return checkPassword();
```

http://192.168.1.1/cgi-bin/luci

```
detectCapsLock(event, 1, 'login')
```

http://192.168.1.1/luci-static/resources/js/login.js

```
//javascript for login.html
var isEmpty = true;
var gLoginFlag = 0;
var bType = BrowserType();
var jumpage = false;

window.localStorage.removeItem("hasWiFi");
window.localStorage.removeItem("hasUsb");

$(document).ready(function(){
 if (window != top)
         top.location.href = "/cgi-bin/luci";

 //change the stylesheet of login
 if ((bType != "IE8") && !jumpage)
        {
         console.log("Current broswer is " + bType);
         showAnimateLine();
        }
 showAnimateTip("login_tip");

 $(".login-block input").focusin(function(){
   $(this).parent(".login-block").addClass("login-block-focused");
 });
 $(".login-block input").focusout(function(){
   $(this).parent(".login-block").removeClass("login-block-focused");
 });

 //       当浏览器窗口高度小于一定时，固定container高度
 $(window).resize(function(){
         var browserHeight =$(window).height();
         if(browserHeight <= 500){
                 $(".login_bg").css("height","500px");

         }else{
                 $(".login_bg").css("height","100%");
                }
     console.log(browserHeight)
 });


 $(".pwd-show-switch").bind("click", function(){
                if($(this).attr("class").indexOf("filled") != -1){
                        if(9 > judedNavation()){
                                var $pwdInput = $(this).parent(".password_block").find("input");
                                if($pwdInput.attr("type").indexOf("password") != -1){
                                        var inputStr = createInput($pwdInput.attr("id"),
$pwdInput.attr("name"), "password", "text", $pwdInput.val(),  $pwdInput.attr("class"));
                                        $pwdInput.replaceWith($(inputStr));
                                        $(this).addClass("open");
                                }else{
                                        var inputStr = createInput($pwdInput.attr("id"),
$pwdInput.attr("name"), "password", "password", $pwdInput.val(),  $pwdInput.attr("class"));
                                        $pwdInput.replaceWith($(inputStr));
                                        $(this).removeClass("open");
                                       }
                        }else{
                                var $pwd_input = $(this).parent(".password_block").find("input");
                         if($pwd_input.attr("type") == "password"){
                                 $pwd_input[0].type = "text";
                                 $(this).addClass("open");
                         }else if($pwd_input.attr("type") == "text"){
                                 $pwd_input[0].type = "password";
                                 $(this).removeClass("open");
                         }else{
                                 $pwd_input[0].type = "password";
                                 $(this).removeClass("open");
                                }
                               }
                }
 });
});
```

```
function showAnimateTip(id)
{
 $("#"+id).animate({
    left: 0
 }, 500);
}

function showAnimateLine()
{
 var speed=6;
    function Marquee(){
      if(document.getElementById("line2").offsetWidth-document.getElementById("line").scrollLeft<=0)
        document.getElementById("line").scrollLeft-=document.getElementById("line1").offsetWidth;
      else{
        document.getElementById("line").scrollLeft++;
      }
    }
        setInterval(Marquee,speed);
}

function judedNavation()
{
 if(navigator.appName == "Microsoft Internet Explorer" && navigator.appVersion.match(/6./i)=="6."){
         return 6;
 }
 else if(navigator.appName == "Microsoft Internet Explorer" &&
navigator.appVersion.match(/7./i)=="7."){
         return 7;
 }
 else if(navigator.appName == "Microsoft Internet Explorer" &&
navigator.appVersion.match(/8./i)=="8."){
         return 8;
 }
 else if(navigator.appName == "Microsoft Internet Explorer" &&
navigator.appVersion.match(/9./i)=="9."){
         return 9;
        }
 else{
         return 10;
        }
}


function createInput(id, name, placeholder, type, value, classname)
{
 var inputObj = "<input ";
 inputObj += "id='" + id + "' ";
 inputObj += "class='" + classname + "' ";
 inputObj += "name='" + name + "' ";
 inputObj += "placeholder='" + placeholder + "' ";
 inputObj += "type='" + type + "' ";
 inputObj += "value='" + value + "' ";
 inputObj += ">";
 return inputObj;
}

function checkPassword()
{
 if ($("#login_password").val().length < 5)
        {
         if ( $("#login_username").parent().parent().children().length > 2)
                 $("#login_username").parent().parent().children(":last").remove();
     $("#login_username").parent().parent().children(":last").after("<div><font face=\"       宋体\"
style=\"font-size: 14px; color:#aaa\">密码长度必须大于等于五个字符</font></div>");

         return false;
        }

 $("#login_username").val("useradmin");

 return true;
}
```

http://192.168.1.1:8080/maintain

```
var g_wlan24_num=8var g_wlan58_num=8var g_usb_num=1var g_province="JT"
```

http://192.168.1.1:8080/maintain

```
    if (g_province == "JT" || g_province == "HAI") {        window.location="/";    } else {
window.location="/register.html";    }
```

http://192.168.1.1:8080/js/aes_1.js

```
var passwd_key = ""
function encryted_pwd(pwd){
 var key = "";
 for(var i = 0; i < passwd_key.length; i++){
         if(passwd_key.charCodeAt(i) < 16){
                 key += ("0" + (passwd_key.charCodeAt(i)).toString(16));
                }
         else{
                 key += (passwd_key.charCodeAt(i)).toString(16);
                }
        }
 if (key.length > 64){
         key = key.slice(0,64);
        }
 else{
         for (var i = key.length; i < 64 ; i++){
                 key += "0";
                }
        }
 key = CryptoJS.enc.Hex.parse(key);
 return en_func(pwd,key);
}

var Crypto_aes_g_key = "6873616E0000000000000000000000000000000000000000000000000000000000000000";

function encrypt_info(pwd){
 var key = CryptoJS.enc.Hex.parse(Crypto_aes_g_key);
 return en_func(pwd,key);
}

function en_func(pwd,key){
 var ivRand = randNum(16);
 pwd = CryptoJS.enc.Utf8.parse(pwd);
 var encryptedPwd = CryptoJS.AES.encrypt(pwd, key, {
     //iv: CryptoJS.enc.Utf8.parse("0000000000000000"),
     iv: CryptoJS.enc.Hex.parse(ivRand),
     mode: CryptoJS.mode.CBC,
     padding: CryptoJS.pad.Pkcs7
 });

 var encryptedPwdStr = encryptedPwd.ciphertext.toString();
 //return encryptedBase64Str;
 var ivEncryptedPwd = ivRand + encryptedPwdStr;
 return ivEncryptedPwd;
}

function randNum(n){
    var rnd = "";
    var rndIv = "";
    for(var i=0;i<n;i++){
        rnd = Math.floor(Math.random()*256);
        if(rnd<16)
                 rnd = "0" + rnd.toString(16);
         else
                 rnd = rnd.toString(16);
         rndIv += rnd;
```

```
    }
    return rndIv;
}

function decrypt_info(encryptedIvPwd){
 var key = CryptoJS.enc.Hex.parse(Crypto_aes_g_key);
 var ivRecived = encryptedIvPwd.slice(0,32);
 var encryptedPwd = encryptedIvPwd.slice(32,encryptedIvPwd.length);
 var encryptedHexStr = CryptoJS.enc.Hex.parse(encryptedPwd);
    var encryptedBase64Str = CryptoJS.enc.Base64.stringify(encryptedHexStr);

    var decryptedData = CryptoJS.AES.decrypt(encryptedBase64Str, key, {
     //iv: CryptoJS.enc.Utf8.parse("0000000000000000"),
     iv: CryptoJS.enc.Hex.parse(ivRecived),
     mode: CryptoJS.mode.CBC,
     padding: CryptoJS.pad.Pkcs7
 });

    var decryptedStr = decryptedData.toString(CryptoJS.enc.Utf8);
    return decryptedStr.toString();
}

var hexMap = new Array('0', '1', '2', '3', '4', '5', '6', '7', '8', '9', 'A', 'B', 'C', 'D', 'E', 'F');

function getDHprvkey(){
 var dhPrvKey = "";
 dhPrvKey += (Math.floor(Math.random() * 15)).toString(16);
 for (var j = 0; j < 191; j++){
         dhPrvKey += (Math.floor(Math.random() * 16)).toString(16);
        }

 return dhPrvKey;
}

function getDHkey(g,n,p){
 var g_Bigint = Bigint.fromHex(g);
 var n_Bigint = Bigint.fromHex(n);
 var p_Bigint = Bigint.fromHex(p);
 var dhKey = Bigint._powmod(g_Bigint,n_Bigint,p_Bigint);
 var dhKey_binary = dhKey.toBinaryString();
 var dhKey_tmp = "";
 var tmp,tmpLen;
 for (var i=dhKey_binary.length-1; i >= 0; i=i-4){
         if ((i-3)<0){
                 tmp = dhKey_binary.slice(0,i+1);
                 tmpLen = 4 - tmp.length;
                 for (var j = 0; j < tmpLen; j++) {
                         tmp = "0" + tmp;
                        }
                }
         else
                 tmp = dhKey_binary.slice(i-3,i+1);
         dhKey_tmp = hexMap[((tmp[0]=='1')?8:0)+((tmp[1]=='1')?4:0)+((tmp[2]=='1')?2:0)+
((tmp[3]=='1')?1:0)] + dhKey_tmp;
        }
 if(dhKey_tmp.length % 2 == 1)
         dhKey_tmp = "0" + dhKey_tmp;
 return dhKey_tmp;
}

function genDHkey(data,privkey,p){
    data = eval("("+data+")");
 if(data.data.web_stuff){
          var keysuff = '', exclus = '', aeskey = '';
          keysuff = getDHkey(data.data.web_stuff, privkey, p);
          var hex1 = 0, hex2 = 0, hex3 = 0, dec = 0, len = keysuff.length/3;
          for(var i = 0; i < len; i+=2){
          hex1 = '0x'+keysuff.slice(i, i+2);
          hex2 = '0x'+keysuff.slice(i+len, i+len+2);
          hex3 = '0x'+keysuff.slice(i+2*len, i+2*len+2);
         dec = hex1 ^ hex2 ^ hex3;
         exclus = dec.toString(16);
         if(exclus.length < 2){
                         exclus = "0" + exclus;
                }
         aeskey += exclus;
     }
     Crypto_aes_g_key = aeskey;
```

```
        }
    else{
        Crypto_aes_g_key = "6873616E0000000000000000000000000000000000000000000000000000000000000000";
    }
}

var CryptoJS=CryptoJS||function(u,p){
 var d={},l=d.lib={},s=function(){},t=l.Base={extend:function(a){
                s.prototype=this;
                var c=new s;
                a&&c.mixIn(a);
                c.hasOwnProperty("init")||(c.init=function(){
                        c.$super.init.apply(this,arguments);
                })       ;
                c.init.prototype=c;
                c.$super=this;
                return c;
        }       ,
        create:function(){
                var a=this.extend();
                a.init.apply(a,arguments);
                return a;
        }       ,
        init:function(){},
        mixIn:function(a){
                for(var c in a)
                        a.hasOwnProperty(c)&&(this[c]=a[c]);
                a.hasOwnProperty("toString")&&(this.toString=a.toString);
        }       ,
        clone:function(){
                return this.init.prototype.extend(this);
               }
 },
 r=l.WordArray=t.extend({
        init:function(a,c){
                a=this.words=a||[];
                this.sigBytes=c!=p?c:4*a.length;
        }       ,
        toString:function(a){
                return (a||v).stringify(this);
        }       ,
        concat:function(a){
                var c=this.words,e=a.words,j=this.sigBytes;
                a=a.sigBytes;
                this.clamp();
                if(j%4)
                        for(var k=0;k<a;k++)
                                c[j+k>>>2]|=(e[k>>>2]>>>24-8*(k%4)&255)<<24-8*((j+k)%4);
                else if(65535<e.length)
...
```

http://192.168.1.1:8080/js/jquery.js

```
/*!
 * jQuery JavaScript Library v3.7.1
 * https://jquery.com/
 *
 * Copyright OpenJS Foundation and other contributors
 * Released under the MIT license
 * https://jquery.org/license
 *
 * Date: 2023-08-28T13:37Z
 */
( function( global, factory ) {

 "use strict";

 if ( typeof module === "object" && typeof module.exports === "object" ) {

        // For CommonJS and CommonJS-like environments where a proper `window`
        // is present, execute the factory and get jQuery.
        // For environments that do not have a `window` with a `document`
        // (such as Node.js), expose a factory as module.exports.
```

```
        // This accentuates the need for the creation of a real `window`.
        // e.g. var jQuery = require("jquery")(window);
        // See ticket trac-14549 for more info.
        module.exports = global.document ?
                factory( global, true ) :
                function( w ) {
                        if ( !w.document ) {
                                throw new Error( "jQuery requires a window with a document" );
                               }
                        return factory( w );
                }       ;
 } else {
         factory( global );
        }

// Pass this if window is not defined yet
} )( typeof window !== "undefined" ? window : this, function( window, noGlobal ) {

// Edge <= 12 - 13+, Firefox <=18 - 45+, IE 10 - 11, Safari 5.1 - 9+, iOS 6 - 9.1
// throw exceptions when non-strict code (e.g., ASP.NET 4.5) accesses strict mode
// arguments.callee.caller (trac-13335). But as of jQuery 3.0 (2016), strict mode should be common
// enough that all such attempts are guarded in a try block.
"use strict";

var arr = [];

var getProto = Object.getPrototypeOf;

var slice = arr.slice;

var flat = arr.flat ? function( array ) {
 return arr.flat.call( array );
} : function( array ) {
 return arr.concat.apply( [], array );
};


var push = arr.push;

var indexOf = arr.indexOf;

var class2type = {};

var toString = class2type.toString;

var hasOwn = class2type.hasOwnProperty;

var fnToString = hasOwn.toString;

var ObjectFunctionString = fnToString.call( Object );

var support = {};

var isFunction = function isFunction( obj ) {

        // Support: Chrome <=57, Firefox <=52
        // In some browsers, typeof returns "function" for HTML <object> elements
        // (i.e., `typeof document.createElement( "object" ) === "function"`).
        // We don't want to classify *any* DOM node as a function.
        // Support: QtWeb <=3.8.5, WebKit <=534.34, wkhtmltopdf tool <=0.12.5
        // Plus for old WebKit, typeof returns "function" for HTML collections
        // (e.g., `typeof document.getElementsByTagName("div") === "function"`). (gh-4756)
        return typeof obj === "function" && typeof obj.nodeType !== "number" &&
                typeof obj.item !== "function";
 };


var isWindow = function isWindow( obj ) {
        return obj != null && obj === obj.window;
 };


var document = window.document;



 var preservedScriptAttributes = {
        type: true,
```

```
        src: true,
        nonce: true,
        noModule: true
};

function DOMEval( code, node, doc ) {
        doc = doc || document;

        var i, val,
                script = doc.createElement( "script" );

        script.text = code;
        if ( node ) {
                for ( i in preservedScriptAttributes ) {

                        // Support: Firefox 64+, Edge 18+
                        // Some browsers don't support the "nonce" property on scripts.
                        // On the other hand, just using `getAttribute` is not enough as
                        // the `nonce` attribute is reset to an empty string whenever it
                        // becomes browsing-context connected.
                        // See https://github.com/whatwg/html/issues/2369
                        // See https://html.spec.whatwg.org/#nonce-attributes
                        // The `node.getAttribute` check was added for the sake of
                        // `jQuery.globalEval` so that it can fake a nonce-containing node
                        // via an object.
                        val = node[ i ] || node.getAttribute && node.getAttribute( i );
                        if ( val ) {
                                script.setAttribute( i, val );
                               }
                       }
               }
        doc.head.appendChild( script ).parentNode.removeChild( script );
       }


function toType( obj ) {
 if ( obj == null ) {
        return obj + "";
       }

 // Support: Android <=2.3 only (functionish RegExp)
 return typeof obj === "object" || typeof obj === "function" ?
        class2type[ toString.call( obj ) ] || "object" :
        typeof obj;
}
/* global Symbol */
// Defining this global in .eslintrc.json would create a danger of using the global
// unguarded in another place, it seems safer to define global only for this module



var version = "3.7.1",

 rhtmlSuffix = /HTML$/i,

 // Define a local copy of jQuery
 jQuery = function( selector, context ) {

        // The jQuery object is actually just the init constructor 'enhanced'
        // Need init if jQuery is called (just allow error to be thrown if not included)
        return new jQuery.fn.init( selector, context );
 };

jQuery.fn = jQuery.prototype = {

 // The current version of jQuery being used
 jquery: version,

 constructor: jQuery,

 // The default length of a jQuery object is 0
 length: 0,

 toArray: function() {
        return slice.call( this );
 },

 // Get the Nth element in the matched element set OR
```

```
 // Get the whole matched element set as a clean array
 get: function( num ) {

         // Return all the elements in a clean array
         if ( num ==...
```

http://192.168.1.1:8080/js/common.js

```
function web_server_result(s) {
 if (s == "null error") {
         return "       某些项的值无效，请重新填写"
 } else if (s == "data error") {
         return "       某些项的值无效，请重新填写"
 } else if (s == "set error") {
         return "       设置失败"
 } else if (s == "add error") {
         return "       添加失败"
 } else if (s == "del error") {
         return "       删除失败"
 } else if (s == "get error") {
         return "       获取配置失败"
 } else {
         return s
        }
}

function common_ajax_success(rsp, status, xhr) {
 var rsp_obj = rsp
 if (typeof(rsp) == "string")
         rsp_obj = JSON.parse(rsp)

 if (typeof(rsp_obj) == "object" && rsp_obj.retcode == "0" && rsp_obj.data.result == "SUCCESS") {
         location.reload()
 } else {
         var msg = ""
         if (rsp_obj.data && rsp_obj.data.errinfo) {
                 msg = msg + web_server_result(rsp_obj.data.errinfo)
                }
         if (rsp_obj.data && rsp_obj.data.result) {
                 msg = msg + rsp_obj.data.result
                }
         if (msg == "") {
                 msg = "       未知的错误"
                }

         pop_window.alert({title:"       警告", text:msg, confirm:true})
        }
}

function common_ajax_success_cb(rsp, status, xhr, cb) {
 var rsp_obj = rsp
 if (typeof(rsp) == "string")
         rsp_obj = JSON.parse(rsp)

 if (typeof(rsp_obj) == "object" && rsp_obj.retcode == "0" && rsp_obj.data.result == "SUCCESS") {
         cb()
 } else {
         var msg = ""
         if (rsp_obj.data && rsp_obj.data.errinfo) {
                 msg = msg + web_server_result(rsp_obj.data.errinfo)
                }
         if (rsp_obj.data && rsp_obj.data.result) {
                 msg = msg + rsp_obj.data.result
                }
         if (msg == "") {
                 msg = "       未知的错误"
                }

         pop_window.alert({title:"       警告", text:msg, confirm:true})
        }
}

function getQueryVariable(variable) {
```

```
    let query = window.location.search.substring(1);
    let vars = query.split("&");
    for (let i = 0; i < vars.length; i++) {
        let pair = vars[i].split("=");
        if (pair[0] == variable) {
          return pair[1];
        }
    }
}

function hasClass (ele, className) {
 var reg = new RegExp('(^|\\s)' + className + '(\\s|$)')
 return reg.test(ele.className)
}

function macToNumber(mac) {
 return Number("0x"+mac.replaceAll(':',''))
}

function ipToNumber(ip) {
 var num = 0;
 if(ip == "") {
         return num;
 }
    var aNum = ip.split(".");
    if(aNum.length != 4) {
        return num;
    }
    num += parseInt(aNum[0]) << 24;
    num += parseInt(aNum[1]) << 16;
    num += parseInt(aNum[2]) << 8;
    num += parseInt(aNum[3]) << 0;
    num = num >>> 0;//这个很关键，不然可能会出现负数的情况
    return num;
}

function numberToIp(number) {
    var ip = "";
    if(number <= 0) {
        return ip;
    }
    var ip3 = (number << 0 ) >>> 24;
    var ip2 = (number << 8 ) >>> 24;
    var ip1 = (number << 16) >>> 24;
    var ip0 = (number << 24) >>> 24

    ip += ip3 + "." + ip2 + "." + ip1 + "." + ip0;

    return ip;
}

function ipv4_prefix(ip) {
 var arr = ip.split('.')
 delete arr[3]
 return arr.join('.')
}

function is_ipv4(ip) {
 return /^(1\d{2}|2[0-4]\d|25[0-5]|[1-9]\d|[0-9])\.((1\d{2}|2[0-4]\d|25[0-5]|[1-9]\d|\d)\.){2}
(1\d{2}|2[0-4]\d|25[0-5]|[1-9]\d|\d)$/.test(ip)
}

function is_ipv6(ip) {
 return /^([\da-fA-F]{1,4}:){6}((25[0-5]|2[0-4]\d|[01]?\d\d?)\.){3}(25[0-5]|2[0-4]\d|[01]?\d\d?)$|^::
([\da-fA-F]{1,4}:){0,4}((25[0-5]|2[0-4]\d|[01]?\d\d?)\.){3}(25[0-5]|2[0-4]\d|[01]?\d\d?)$|^([\da-fA-F]
{1,4}:):([\da-fA-F]{1,4}:){0,3}((25[0-5]|2[0-4]\d|[01]?\d\d?)\.){3}(25[0-5]|2[0-4]\d|[01]?\d\d?)$|^([\da-fA-
F]{1,4}:){2}:([\da-fA-F]{1,4}:){0,2}((25[0-5]|2[0-4]\d|[01]?\d\d?)\.){3}(25[0-5]|2[0-4]\d|[01]?
\d\d?)$|^([\da-fA-F]{1,4}:){3}:([\da-fA-F]{1,4}:){0,1}((25[0-5]|2[0-4]\d|[01]?\d\d?)\.){3}(25[0-5]|2[0-4]\d|
[01]?\d\d?)$|^([\da-fA-F]{1,4}:){4}:((25[0-5]|2[0-4]\d|[01]?\d\d?)\.){3}(25[0-5]|2[0-4]\d|[01]?
\d\d?)$|^([\da-fA-F]{1,4}:){7}[\da-fA-F]{1,4}$|^:((:[\da-fA-F]{1,4}){1,6}|:)$|^[\da-fA-F]{1,4}:((:[\da-fA-F]
{1,4}){1,5}|:)$|^([\da-fA-F]{1,4}:){2}((:[\da-fA-F]{1,4}){1,4}|:)$|^([\da-fA-F]{1,4}:){3}((:[\da-fA-F]{1,4})
{1,3}|:)$|^([\da-fA-F]{1,4}:){4}((:[\da-fA-F]{1,4}){1,2}|:)$|^([\da-fA-F]{1,4}:){5}:([\da-fA-F]{1,4})?
$|^([\da-fA-F]{1,4}:){6}:$/.test(ip)
}

function is_domain(domain) {
 return /^(?=^.{3,255}$)[a-zA-Z0-9][-a-zA-Z0-9]{0,62}(\.[a-zA-Z0-9][-a-zA-Z0-9]{0,62})+$/.test(domain)
}
```

```
function is_hex(s) {
 for (var i in s) {
         if (!((s[i].charCodeAt() >= '0'.charCodeAt() && s[i].charCodeAt() <= '9'.charCodeAt()) ||
                 (s[i].charCodeAt() >= 'a'.charCodeAt() && s[i].charCodeAt() <= 'f'.charCodeAt()) ||
                 (s[i].charCodeAt() >= 'A'.charCodeAt() && s[i].charCodeAt() <= 'F'.charCodeAt())))
                {
                 return false
                }
        }

 return true
}

function iform_data() {
    var data = {}
    $.each($("iform select:enabled"), function(i, select){
        data[select.name] = select.value
    })
    $.each($("iform input:enabled"), function(i, input){
         if (input.type != "button") {
                 if (input.type == "checkbox") {
                         data[input.name] = input.checked ? "1" : "0"
                 } else {
                         data[input.name] = input.value
                        }
                }
    })
    return data
}

function iform_data_id(id) {
    var data = {}
    $.each($("#"+id+" select:enabled"), function(i, select){
        data[select.name] = select.value
    })
    $.each($("#"+id+" input:enable...
```

http://192.168.1.1:8080/login.html

```
var is_80_login = falsevar login_err = getQueryVariable("login_err")var username =
getQueryVariable("username")var psd = getQueryVariable("psd")$(document).ready(function(){//海南电信需求：新增路
由设置功能if (g_province == "HAI") {$("#route_set_span").show()$.ajax({url:
'/boaform/global_attr_get.cgi',type: 'post',success: function(rsp, status, xhr){var data =
JSON.parse(rsp).dataif (data.ulRouteStatus == "0") {$("#route_set_span input").attr("disabled",
false)}},})}//非集团版本，显示注册按钮。注册成功后禁用注册按钮if (g_province != "JT")
{$("#register_span").show()$.ajax({url: '/boaform/web_Capability_show.cgi',type: 'post',success:
function(rsp, status, xhr){var data = JSON.parse(rsp).dataif (!(data.g_status == "0" && data.g_result ==
"1")) {$("#register_span input").attr("disabled", false)}},})if (login_err) {is_80_login =
truelogin_err_info(login_err)} else {if (username && psd) {psd = decodeURI(psd)is_80_login =
truelogin()}}})function login_hint(msg){pop_window.alert({title:"登入提
示",text:msg,confirm:true,close:function(){if (is_80_login)window.location = location.protocol + "//" +
location.hostname;},})}function login_err_info(err) {if (err == "success_telecomadmin") {window.location =
"/admin/status_overview_ip.html";} else if (err == "success_useradmin") {login_hint("账号或密码错误，请重新登
录！")} else if(err == "invalid_username") {login_hint("账号或密码错误，请重新登录！")} else if(err ==
"bad_password"){login_hint("账号或密码错误，请重新登录！")} else if(err == "invalid_password"){login_hint("账号或密
码错误，请重新登录！")} else if(err == "three_error_login") {login_hint("密码错误三次，请一分钟之后重新登录！")} else
if (err == "one_user_login") {login_hint("当前已有一个用户已登陆，退出已登陆用户重试！");} else if (err ==
"telecomadmin_disabled_err") {login_hint("维护账号使能未打开！");} else {login_hint("未知的错误");}}function
createXmlhttp () {if (window.XMLHttpRequest) {//针对FireFox，Mozillar，Opera，Safari，IE7，IE8xmlhttp = new
XMLHttpRequest();//针对某些特定版本的mozillar浏览器的BUG进行修正if (xmlhttp.overrideMimeType) {
xmlhttp.overrideMimeType("text/xml");   }}else if (window.ActiveXObject) {//针对IE6，IE5.5，IE5//两个可以用于创建
XMLHTTPRequest对象的控件名称，保存在一个js的数组中//排在前面的版本较新var activexName =
["MSXML2.XMLHTTP","Microsoft.XMLHTTP"];for (var i = 0; i < activexName.length; i++) {try{//取出一个控件名进行创
建，如果创建成功就终止循环//如果创建失败，回抛出异常，然后可以继续循环，继续尝试创建xmlhttp = new
ActiveXObject(activexName[i]);break;} catch(e){}}}}function sendRequest(url,param,callback){createXmlhttp
();try{//xmlhttp.onreadystatechange = processResponse;  //回调方法xmlhttp.open("post",url ,false); // true异步
xmlhttp.setRequestHeader("content-type","application/x-www-form-urlencoded");xmlhttp.setRequestHeader("Cache-
Control", "no-cache");var str = ''for(var i in param){str += i + "=" + encodeURIComponent(param[i]) +
"&";}str = str.substring(0,str.length -1);xmlhttp.send(str);var str = xmlhttp.responseText;var webdata =
eval("("+str+")");if (webdata){webdata = webdata.data;}if(callback){callback(webdata);}}catch(e){}}function
route_set() {window.location = "/route_set.html"}function login() {var dataif (is_80_login) {data =
{web_login_name: username,web_login_password: psd,}} else {data = {web_login_name:
```

```
document.getElementById("login_username").value,web_login_password:
document.getElementById("login_password").value,}data.web_login_name = (data.web_login_name == "useradmin" ?
"telecomadmin" : data.web_login_name)data.web_login_password =
data.web_login_password}sendRequest('/boaform/passwd_key_show.cgi', {}, function(d1){passwd_key =
d1.passwd_keydata.web_login_password =
encryted_pwd(data.web_login_password)sendRequest('/boaform/web_login_exe.cgi', data, function(d2)
{login_err_info(d2.result)})})}function reset()
{$("#login_username").val("useradmin")$("#login_password").val("")}function register() {window.location =
"http://192.168.1.1:8080/register.html"}
```

http://192.168.1.1:8080/login.html

```
route_set()
```

http://192.168.1.1:8080/login.html

```
login()
```

http://192.168.1.1:8080/login.html

```
reset()
```

http://192.168.1.1:8080/login.html

```
register()
```

cookie 0

TOC

名称	首先设置	域	安全
值	请求的 URL		到期