

New issue

Jump to bottom

[Bug]普通用户可上传插件至任意代码执行 #2431

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

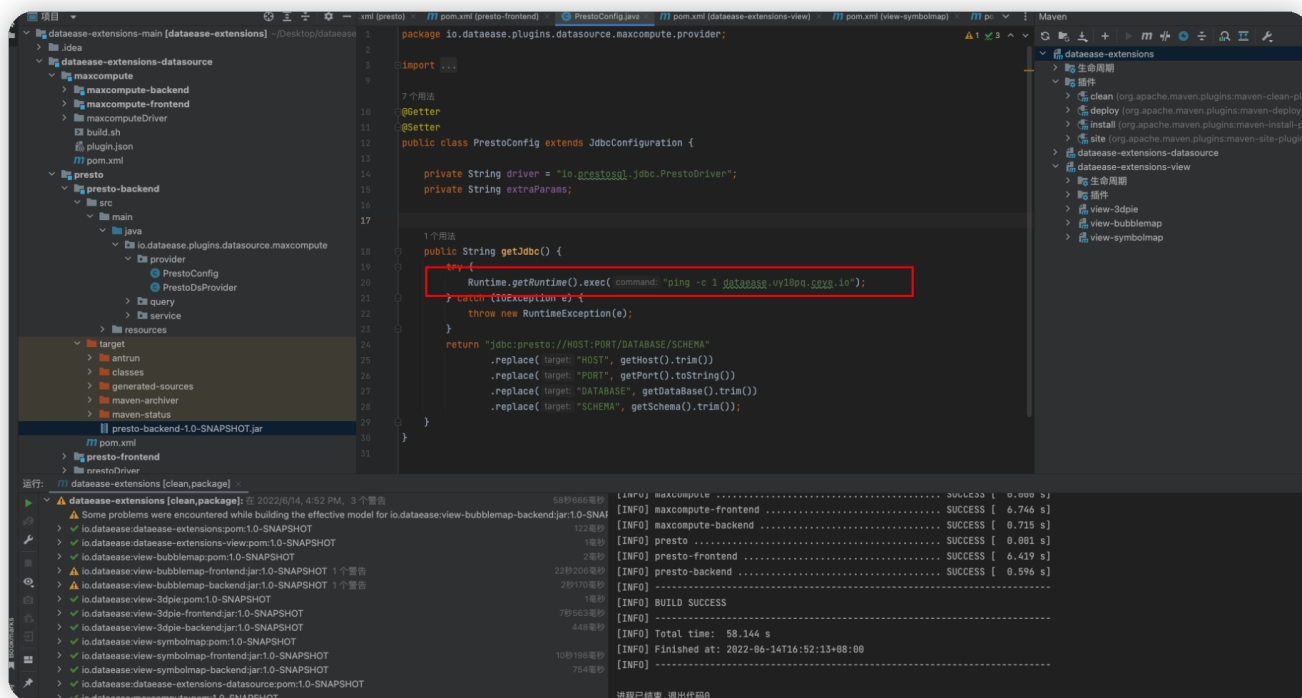
运行方式(安装包运行 or 源码运行 ?)
安装包运行

浏览器版本
任意

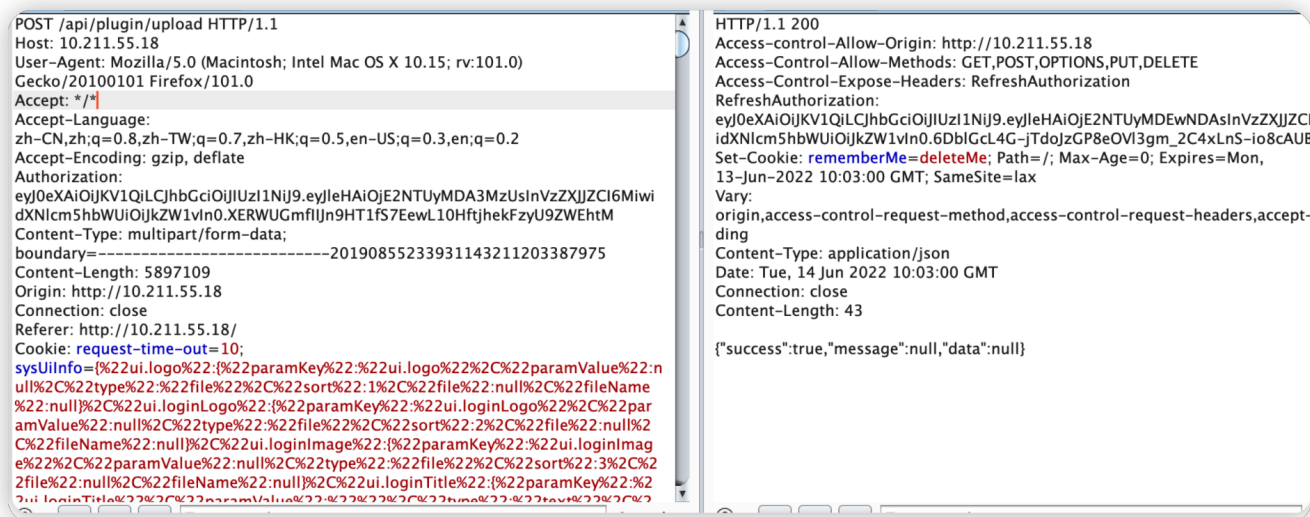
Bug 描述
普通用户可上传插件至任意代码执行

Bug 重现步骤(有截图更好)

在官网编译插件，并在主要连接presto的功能处加入恶意代码：



插件安装处未鉴权，普通用户可调用接口上传插件：



上传成功后普通用户新建presto数据源：

DataEase

首页

仪表板

数据集

数据源

系统管理

demo

数据源

+ 新建数据源

驱动管理

搜索

MySQL

← 新建数据源

* 名称

123

描述

* 类型

Presto

驱动

Default

* 主机名

127.0.0.1

* 端口

123

* 数据库

123

* Schema

123

* 用户名

123

密码

校验

保存

查看dnslog平台：

ID	Name	Remote Addr
671491089	dataease.uy10pq.ceye.io	
671491079	dataease.uy10pq.ceye.io	
671491037	dataease.uy10pq.ceye.io	
671491036	dataease.uy10pq.ceye.io	
671491035	dataease.uy10pq.ceye.io	

命令成功执行

  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]普通用户可上传插件至任意代码执行 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

