

CVE-2020-7799: FreeMarker模板FusionAuth RCE复现

原创  Timeline Sec

2020-06-27原文

收录于话题

#漏洞复现文章合集

70个

点击上方蓝色字体关注我们，一起学安全！

本文作者：  (团队复现组成员)

本文字数： 718

阅读时长： 2~3min

声明：请勿用作违法用途，否则后果自负

0x01 简介

FusionAuth是一个免费的身份管理平台，安装简单，易于集成。FusionAuth提供登录、注册、MFA、SSO、电子邮件模板、本地化、密码控制、强哈希、网络挂钩、基于角色的访问控制等功能。

0x02 漏洞概述

一个有修改 email 或者 theme 模板权限的用户可以通过使用 Apache FreeMarker engine 里的 `freemarker.template.utility.Execute` 来执行任意命令。

因为使用了 Apache FreeMarker engine(freemarker-2.3.28.jar), 所以可以使用 freemarker 的语法, 类似 `${XXX? Built-ins}` 而 new 这个 Built-ins 会 创建一个特定 TemplateModel 的 变量。

要求 ? 左边 是 TemplateModel, 也就是 freemarker.template.utility.Execute, 而 右边 就是 initialize 这个 object 时的参数。

0x03 影响版本

FusionAuth <= 1.11.0

0x04 环境搭建

下载 FusionAuth 1.10.0 (本次使用 FusionAuth 1.10.0 进行测试)

https://storage.googleapis.com/inversoft_products_j098230498/products/fusionauth/1.10.0/fusionauth-app-1.10.0.zip

1. 将文件解压之后随便放一个位置
2. 启动 MySQL `/etc/init.d/mysql start`
3. 启动 ElasticSearch `systemctl start elasticsearch.service`
4. 启动 FusionAuth `bin/startup.sh`

```
Downloading Java
##### 100.0%
Starting fusionauth-search ... skipped, not installed
Starting fusionauth-app ... done.
```

5. 打开网址 `http://127.0.0.1:9011/` 配置 FusionAuth

a. 先配置数据库


Maintenance Mode

Database type

FusionAuth is in maintenance mode because your database is not ready, it is either missing tables.

Database type mysql
 postgresql

Host* localhost

Port*  3306

Database* fusionauth

TLS enabled



Superuser credentials

Provide your existing database superuser username and password. This information will be used to create the FusionAuth database. If you do not know the database superuser credentials, you will need to create a new database.

This username and password will only be used during this database configuration step.

Username* kali

Password kali

FusionAuth credentials

Provide a new username and password to own the FusionAuth database. This data will be used to create the FusionAuth database.

b. 配置 Elastic Search

Maintenance Mode

Elasticsearch

FusionAuth is in maintenance mode because your search engine is not ready, it is either not running or your configuration is not complete. Ensure Elasticsearch is running and verify the connection information below.

Servers* ⓘ

[→ Submit](#)

c. 创建好用户之后就可以登录了

Login

[Forgot your password?](#)

English ▾


The screenshot shows the FusionAuth dashboard interface. On the left is a dark sidebar with the FusionAuth logo and a user profile for 'kali kali'. The main content area has a search bar at the top and a 'Dashboard Home' header. Below the header is a 'Complete setup' section containing two task cards: '#1 Missing Application' with a 'Setup' button and '#2 Missing API Key' with an 'Add' button. The top right of the dashboard includes 'Help' and 'Logout' links.

0x05 漏洞复现


本次使用 email template 进行测试


1. 进入 setting -> email template


 System


 Tenants


 Groups

 API Keys

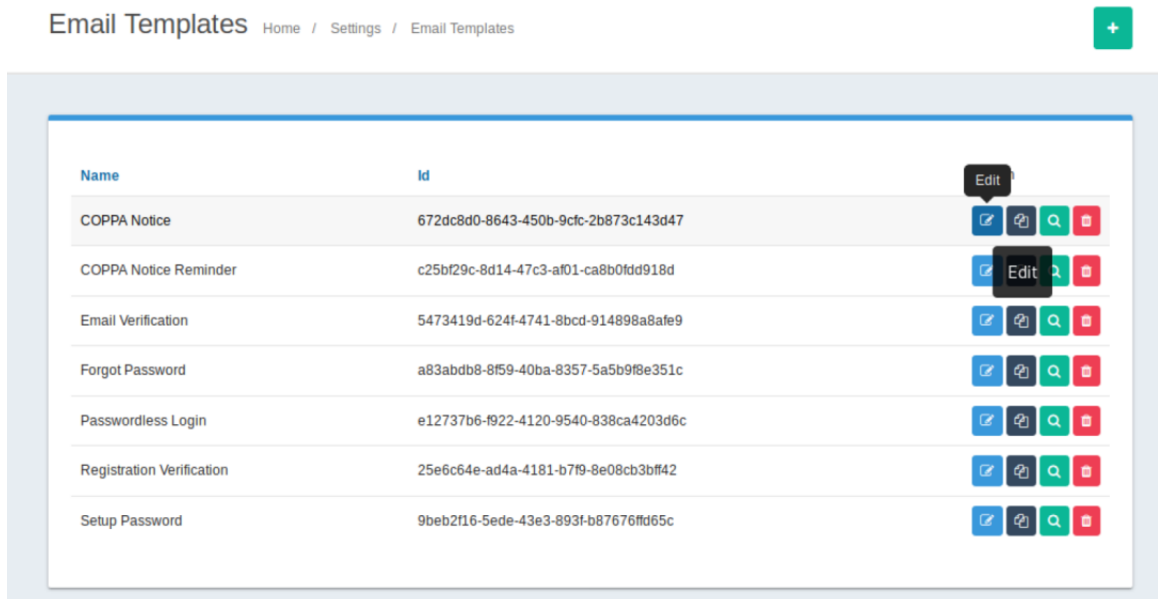
 Lambdas

 Key Master

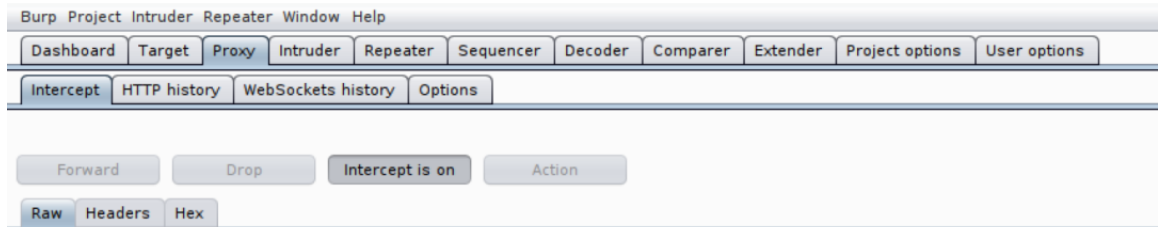
 Identity Providers

 Email Templates

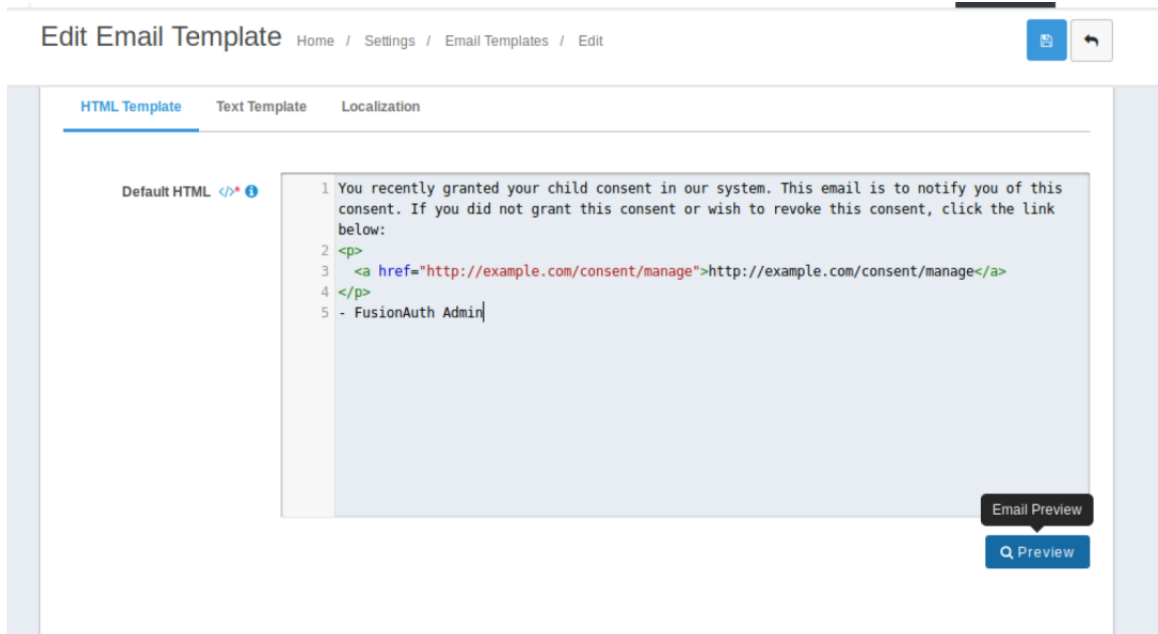
2. 随便点一个 template 的 edit



3. 开启 Burp Suite 抓包, 配置好 proxy



4. 点击 Preview, 然后去 Burp Suite 看抓包



5. 修改

emailTemplate.defaultHtmlTemplate

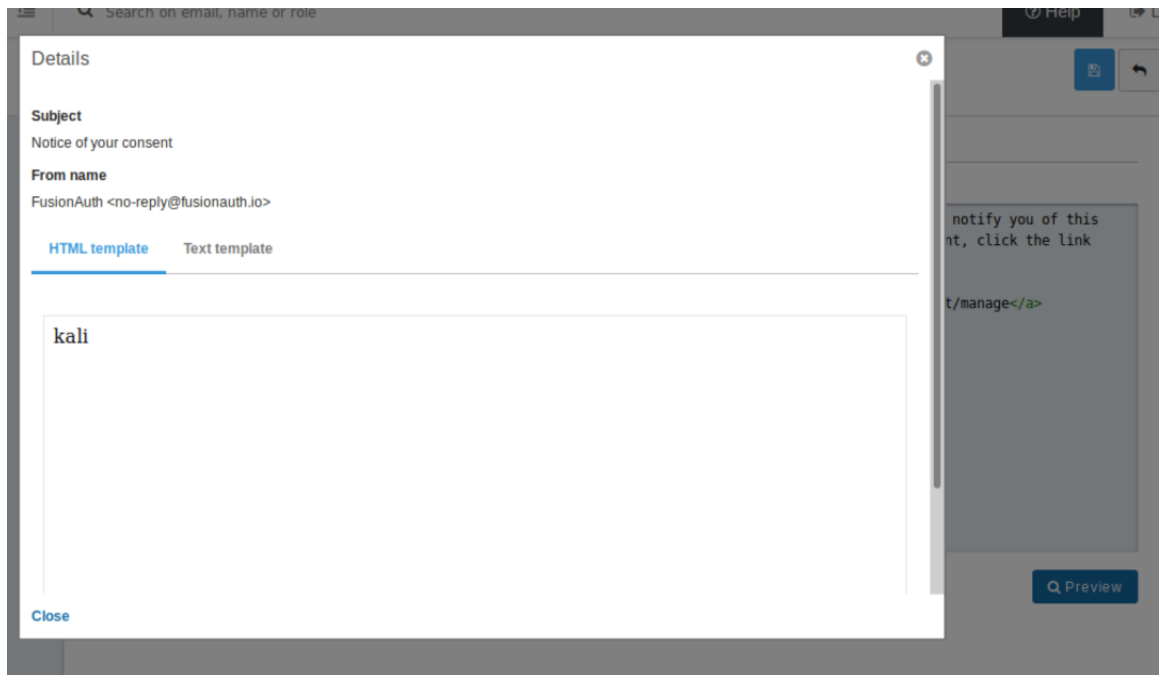
为

```

${"freemarker.template.utility.Execute"?new()}("whoami")

```

6. forward 之后看结果



0x06 修复方式

值得一提的是 freemarker 2.3.19 的 changelog 里显示,如果用户开启了 `TemplateClassResolver.SAFER_RESOLVER` 的话,可以防止创建 `freemarker.template.utility.Execute`. 然而目前这并不是默认配置。

FusionAuth Version 1.11.0 的 release Note 里说是修改了 freemarker template engine,使其不能执行恶意代码. 所以修复方式就是升级到1.11.0 及以后的版本。

参考链接:

<https://www.anquanke.com/post/id/198036>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7799>





阅读原文看更多复现文章

Timeline Sec 团队

安全路上，与你并肩前行

精选留言

用户设置不下载评论

[阅读全文](#)