河南省教育信息安全监测中心
关于开源云存储软件 ownCloud
存在三个高危漏洞的安全风险预警

河南省教育信息安全监测中心
Henan Provincial Education Information Security Monitoring Center

2023 年 12 月 28 日

关于开源云存储软件 ownCloud 存在三个高危漏洞的安全风险预警

事件描述

ownCloud 是一种广泛使用的用于文件共享和内容协作的开源软件，它支持在线文档编辑以及日历和联系人同步等扩展，用户可以通过网络浏览器或各种客户端应用程序访问数据和文档。

ownCloud 官网于 11 月 21 日公布了三个高危漏洞。**一是**信息泄露漏洞(CVE-2023-49103)；**二是**子域验证绕过漏洞(CVE-2023-49104)；**三是**身份验证绕过漏洞(CVE-2023-49105)。

漏洞编号

CVE-2023-49103

CVE-2023-49104

CVE-2023-49105

漏洞危害

高危

受影响版本

1. CVE-2023-49103：

ownCloud/graphapi 0.2.x < 0.2.1

ownCloud/graphapi 0.3.x < 0.3.1

2. CVE-2023-49104:

ownCloud/oauth2 < 0.6.1

3. CVE-2023-49105:

10.6.0 <=ownCloud/core< 10.13.1

漏洞介绍

1. ownCloud 信息泄露漏洞(CVE-2023-49103)

由于 ownCloud graphapi 应用程序依赖于提供 URL 的第三方 GetPhpInfo.php 库，访问特定链接(*http://XXXXXXXXX/ownCloud/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php*)即可获取 PHP 环境的配置详情 (phpinfo)，这些信息包括网络服务器的所有环境变量。在容器化部署中，这些环境变量可能包括敏感数据，如 ownCloud 管理员密码、邮件服务器凭据和许可证密钥等，导致敏感信息泄露。

2. ownCloud 子域验证绕过漏洞(CVE-2023-49104)

   ownCloud oauth2 中，如果用户启用了“允许子域”选项，攻击者能够传入绕过验证的恶意的重定向 URL，从而允许攻击者将用户引导至攻击者控制的顶级域。

3. ownCloud WebDAV API 身份验证绕过漏洞(CVE-2023-49105)

   在 10.13.1 之前的 ownCloud/core 中，默认用户未配置签名密钥，如果已知受害者的用户名，则可使用预签名 URI 绕过 WebDAV Api 身份验证，无需身份验证即可访问、修改或删除任何文件。

修复方案

1. ownCloud 信息泄露漏洞(CVE-2023-49103)

   删除 owncloud/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php 文件，禁用 Docker 容器中的 phpinfo 函数，并更改可能泄露的秘钥（如 ownCloud 管理员密码、邮件服务器和数据库凭据以及 Object-Store/S3 访问密钥）。

2. ownCloud 子域验证绕过漏洞(CVE-2023-49104)

在 Oauth2 应用程序的验证代码中添加加固措施，禁用“允许子域”选项以禁用此漏洞。

3. ownCloud WebDAV API 身份验证绕过漏洞(CVE-2023-49105)

如果文件所有者未配置签名密钥，建议拒绝使用预签名 URL。

4. 详细修复建议请关注官方安全公告。

地址：https://owncloud.com/security/

联系方式

地址：河南省郑州市二七区大学路 75 号郑州大学南校区逸夫楼西

电话：0371-67761893、0371-67765016

传真：0371-67763770

邮箱：hercert@ha.edu.cn

邮编：450052