2023-10-30-CVE-2023-22518-Confluence中的不当授权漏洞

漏洞概述

概述	Confluence中的不当授权漏洞
发布日期	30 Oct 2023
影响产品	• Confluence Data Center • Confluence Server
CVE ID	CVE-2023-22518
官方说明	• CONFSERVER-93

Confluence Data Center和Server的所有版本都受到此未利用漏洞的影响。

可公开访问的Confluence数据中心和服务器版本存在严重风险。

漏洞成因

软件架构中，包的继承和命名空间的使用提供了强大的灵活性，但也带来了潜在的安全风险。当子包继承父包时，它们也继承了父包的接口，但并不总是继承相关的安全控制。
在 Confluence 这个案例中，Confluence 滥用了 Struts2 的继承关系，从而导致可以一定程度绕过它自身的权限校验，最终通过部分接口串联利用实现无需认证的远程代码执行。

漏洞影响

成功利用这个漏洞的攻击者可以在一定程度上绕过身份验证，而后可以通过串联后台接口，无需认证即可控制并且接管服务器。**需要特别注意的是，该漏洞利用会导致 Confluence 数据清空，对应用数据完整性产生不可逆的影响。**

解决方案

临时缓解方案

备份 Confluence 应用数据。如非必要，不要将 Confluence 放置在公网上。或通过网络ACL策略限制访问来源，例如只允许来自特定IP地址或地址段的访问请求。

另外，考虑不使用备份和恢复 功能的话，可以禁用以下功能，可通过修改<install_dir>/confluence/WEB-INF/web.xml中增加以下参数

```
<security-constraint>
                <web-resource-collection>
                        <url-pattern>/json/setup-restore.action</url-pattern>
                        <url-pattern>/json/setup-restore-local.action</url-pattern>
                        <url-pattern>/json/setup-restore-progress.action</url-pattern>
                        <http-method-omission>*</http-method-omission>
                </web-resource-collection>
        <auth-constraint />
</security-constraint>
```

如果有前端nginx，可以配置nginx拦截

```
server {

 ...........

  if ($request_uri ~* "/json/setup-restore.action") {

    return 403;

  }

  if ($request_uri ~* "/json/setup-restore-local.action") {

    return 403;

  }

  if ($request_uri ~* "/json/setup-restore-progress.action") {

    return 403;

  }

  ...........

}
```

升级修复方案

官方已经推出了安全修复版本，强烈建议所有受影响的用户尽快访问官方网站下载安装新版本修复漏洞。

- 7.19.16 or later
- 8.3.4 or later
- 8.4.4 or later
- 8.5.3 or later
- 8.6.1 or later

漏洞扫描工具

点击下载：scanner.zip