security-assessment.com

Vulnerability Advisory

Name	Oracle Siebel eBusiness Application – Multiple Cross Site Scripting Vulnerabilities
Vendor Website	http://www.oracle.com/us/products/applications/ebusiness/index.html
Date Released	18th October 2010 – CVE-2010-2406
Affected Software	Oracle Siebel Suite 7.7.2.12, 7.8.2.14, 8.0.0.10, 8.1.1.3
Researcher	Roberto Suggi Liverani – roberto.suggi@security-assessment.com

Description

Security-Assessment.com has discovered that two components of the Siebel eBusiness Application Suite are vulnerable to reflected Cross Site Scripting attacks. The vulnerabilities can be exploited by both authenticated and unauthenticated remote users.

The following components have been found vulnerable:

- Siebel Web Engine;
- Siebel eBusiness Search Center.
-

Exploitation

The table below details where Cross Site Scripting was detected and which parameters are vulnerable:

Page Affected	Method	Variable
Siebel Web Engine - Public page: /eservice**/"><script>alert(‘xss’)</script>.swe**?SWECmd=Login&SWECM=S Some Siebel eBusiness Applications require the attacker to change the injection using variations such as ">,‘>, %22%3E, ‘}, ‘) .	GET	URL parameter replacing start.swe
Siebel eBusiness Search Center - Only authenticated user can access this page: /start.swe?Id=**%22%3E%3Cscript%3Ealert%28213%29%3C%2Fscript%3E**&SWEField=s_2_1_0_0&SWEFo=SWEForm2_0&SWENeedContext=true&SWESP=false&SWERowIds=&SWEMethod=Find&SWECmd=InvokeMethod&SWEVI=Search&SWEPOC=&SWETF=Search&SWETargetView=&SWEDIC=false&SWEReqRowId=0&SWEView=Find+View&SWETVI=&SWERowId=VRId-0&SWEC=4&SWEM=&SWEBID=1202770071&SWESPa=&SWEContainer=&SWETS=1202773765109&SWETA=&SWEApplet=Find+Applet	GET, POST	Id

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 Oracle eBusiness Suite to upgrade to the latest version as soon as possible. For more information on the new release of Oracle eBusines Suite patch please refer to the release notes:

http://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1210593.1

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