

Scan Results

03/26/2008

The scan was started on 03/25/2008 at 23:39:31 and took 00:31:23 to complete. The scan was run against the following IP addresses:

IP Addresses

68.178.172.38

The scan option profile used includes:

Scan Settings

| | |
|--|---------------|
| Scanned TCP Ports | Full |
| Scanned UDP Ports | Standard Scan |
| Scan Dead Hosts | Off |
| Load Balancer Detection | Off |
| Password Brute Forcing | Standard |
| Vulnerability Detection | Complete |
| Windows Authentication | Disabled |
| SSH Authentication | Disabled |
| Oracle Authentication | Disabled |
| SNMP Authentication | Disabled |
| Perform 3-way Handshake | Off |
| Overall Performance | Custom |
| Hosts to Scan in Parallel-External Scanner | 15 |
| Hosts to Scan in Parallel-Scanner Appliances | 15 |
| Processes to Run in Parallel-Total | 10 |
| Processes to Run in Parallel-HTTP | 10 |
| Packet (Burst) Delay | Medium |

Advanced Settings

| | |
|---|-------------------|
| Host Discovery | TCP Standard Scan |
| | UDP Standard Scan |
| | ICMP On |
| Ignore RST packets | Off |
| Ignore firewall-generated SYN-ACK packets | Off |
| ACK/SYN-ACK packets during discovery | Send |

Report Summary

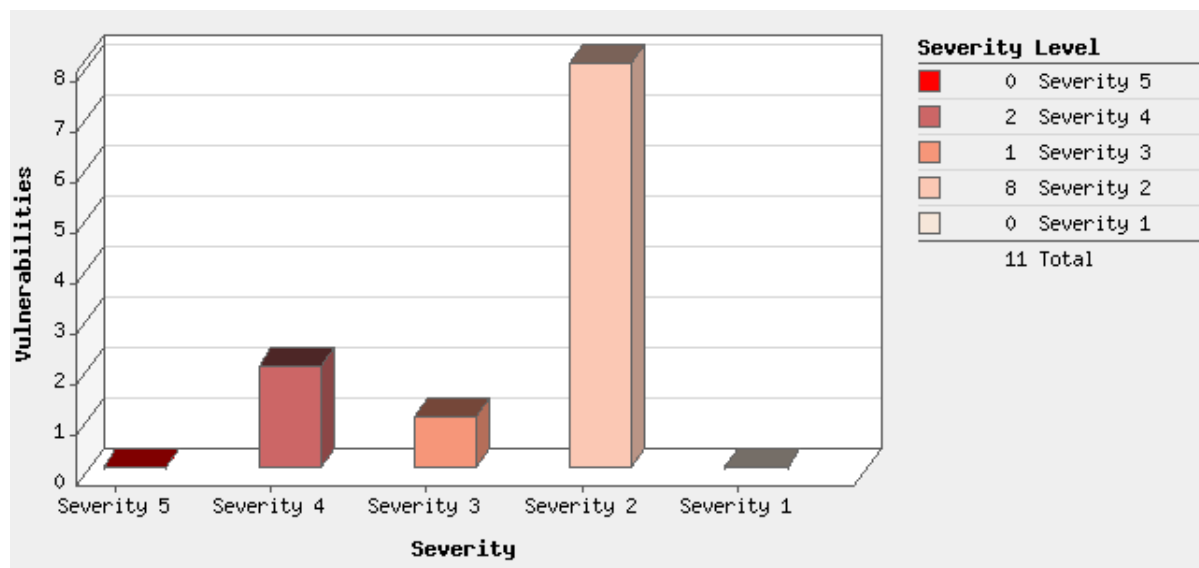
| | |
|--------------------|---|
| Company: | GoDaddy Test Account |
| User: | David Koopman |
| Template Title: | Scan Results |
| Active Hosts: | 1 |
| Total Hosts: | 1 |
| Scan Type: | On Demand |
| Scan Status: | Finished |
| Scan Title: | ModPHP1 |
| Scan Date: | 03/25/2008 at 23:39:31 (GMT) |
| Reference: | scan/1206488374.17761 |
| Scanner Appliance: | 64.39.104.60 (Scanner 4.9.48-1, Web 5.1 FR4 [build 6.1.22-1], Vulnerability Signatures 1.19.98-2) |
| Duration: | 00:31:23 |
| Options: | Payment Card Industry (PCI) Options |
| Target: | 68.178.172.38 |

Summary of Vulnerabilities

| | | | | |
|-----------------------|----|-----------------------|---|-----|
| Vulnerabilities Total | 24 | Average Security Risk |  | 4.0 |
|-----------------------|----|-----------------------|---|-----|

| by Severity | | | | |
|-------------|-----------|-----------|----------------------|-------|
| Severity | Confirmed | Potential | Information Gathered | Total |
| 5 | 0 | 0 | 0 | 0 |
| 4 | 2 | 1 | 0 | 3 |
| 3 | 1 | 1 | 0 | 2 |
| 2 | 8 | 0 | 2 | 10 |
| 1 | 0 | 0 | 9 | 9 |
| Total | 11 | 2 | 11 | 24 |

Vulnerabilities by Severity



Potential Vulnerabilities by Severity

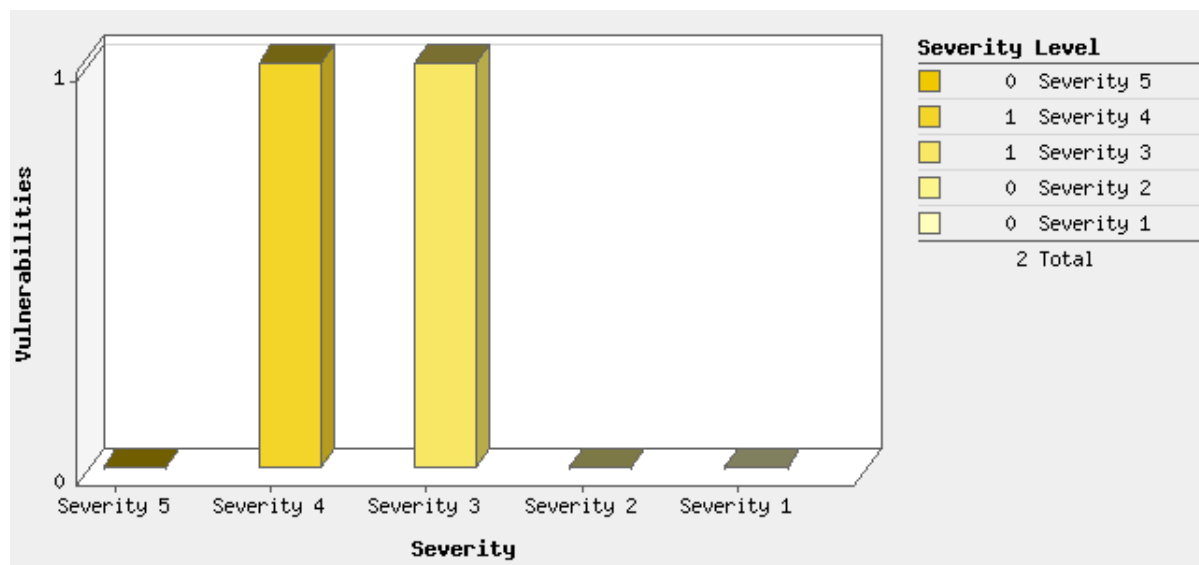


Table of Contents

| | |
|--------------------|---|
| 68.178.172.38..... | 5 |
|--------------------|---|

Detailed Results

68.178.172.38 (ip-68-178-172-38.ip.secureserver.net,-)

Linux 2.4-2.6

Vulnerabilities Total

24

Security Risk



4.0

Compliance Status



FAILED

Vulnerabilities (11)



4

File .htaccess Accessible

port 443/tcp

| | | | |
|-------------------|-------------------------------|----------------|-----|
| QID: | 10177 | CVSS Base: | 3.3 |
| Category: | CGI | CVSS Temporal: | 2.9 |
| CVE ID | CVE-2000-0234 | | |
| Vendor Reference: | - | | |
| Bugtraq ID | 1083 | | |
| Last Update: | 11/30/2005 | | |

THREAT:

.htaccess contains authentication information.

IMPACT:

Unauthorized users can gather authentication information from this file.

SOLUTION:

Change the Apache configuration so the .htaccess file cannot be accessed via the Internet.

RESULT:

```
##
# @version $Id: htaccess.txt 9795 2008-01-02 11:33:07Z rmuilwijk $
# @package Joomla
# @copyright Copyright (C) 2005 - 2008 Open Source Matters. All rights reserved.
# @license http://www.gnu.org/copyleft/gpl.html GNU/GPL
# Joomla! is Free Software
##

#####
# READ THIS COMPLETELY IF YOU CHOOSE TO USE THIS FILE
#
# The line just below this section: 'Options +FollowSymLinks' may cause problems
# with some server configurations. It is required for use of mod_rewrite, but may already
# be set by your server administrator in a way that disallows changing it in
# your .htaccess file. If using it causes your server to error out, comment it out (add # to
# beginning of line), reload your site in your browser and test your self url's. If they work,
# it has been set by your server administrator and you do not need it set here.
#
# Only use one of the two SEF sections that follow. Lines that can be uncommented
# (and thus used) have only one #. Lines with two #'s should not be uncommented
# In the section that you don't use, all lines should start with #
#
#####

## Can be commented out if causes errors, see notes above.
Options +FollowSymLinks

#
# mod_rewrite in use

RewriteEngine On

# Uncomment following line if your webserver's URL
# is not directly related to physical file paths.
# Update Your Joomla! Directory (just / for root)

# RewriteBase /
```

```
##### Begin - Joomla! core SEF Section
#
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteCond %{REQUEST_URI} !^/index.php
RewriteCond %{REQUEST_URI} (/|\.php|\.html|\.htm|\.feed|\.pdf|\.raw|/[\^\.]*)$ [NC]
RewriteRule (.*) index.php
RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization},L]
#
##### End - Joomla! core SEF Section
```

```
##### Begin - Rewrite rules to block out some common exploits
## If you experience problems on your site block out the operations listed below
## This attempts to block the most common type of exploit `attempts` to Joomla!
#
# Block out any script trying to set a mosConfig value through the URL
RewriteCond %{QUERY_STRING} mosConfig_[a-zA-Z]{1,21}(=|\%3D) [OR]
# Block out any script trying to base64_encode crap to send via URL
RewriteCond %{QUERY_STRING} base64_encode.*(.*?) [OR]
# Block out any script that includes a <script> tag in URL
RewriteCond %{QUERY_STRING} (<|\%3C).*script.*(>|\%3E) [NC,OR]
# Block out any script trying to set a PHP GLOBALS variable via URL
RewriteCond %{QUERY_STRING} GLOBALS(=|\\|'|"%[0-9A-Z]{0,2}) [OR]
# Block out any script trying to modify a _REQUEST variable via URL
RewriteCond %{QUERY_STRING} _REQUEST(=|\\|'|"%[0-9A-Z]{0,2})
# Send all blocked request to homepage with 403 Forbidden error!
RewriteRule ^(.*)$ index.php [F,L]
#
##### End - Rewrite rules to block out some common exploits
```

```
# set the spam_ref variable
SetEnvIfNoCase Referer "musicforum.org.ua" spam_ref=1
SetEnvIfNoCase Referer "all-for-women.com" spam_ref=1
SetEnvIfNoCase Referer "detoxonline.org" spam_ref=1
SetEnvIfNoCase Referer "financereal.info" spam_ref=1
SetEnvIfNoCase Referer "health-db.com" spam_ref=1
SetEnvIfNoCase Referer "homes-db.com" spam_ref=1
SetEnvIfNoCase Referer "musicforum.org.ua" spam_ref=1
SetEnvIfNoCase Referer "all-for-women.com" spam_ref=1
SetEnvIfNoCase Referer "mp3clank.com" spam_ref=1
SetEnvIfNoCase Referer "music-db.org" spam_ref=1
SetEnvIfNoCase Referer "musicforum.org.ua" spam_ref=1
SetEnvIfNoCase Referer "1000000mp3.info" spam_ref=1
SetEnvIfNoCase Referer "newmusiccentre.co.uk" spam_ref=1
SetEnvIfNoCase Request_URI "postid=" spam_ref=1
# block all referres that have spam_ref set
<FilesMatch "(.*)">
Order Allow,Deny
Allow from all
Deny from env=spam_ref
</FilesMatch>
```



4 File .htaccess Accessible

port 80/tcp

| | | | |
|-------------------|-------------------------------|----------------|-----|
| QID: | 10177 | CVSS Base: | 3.3 |
| Category: | CGI | CVSS Temporal: | 2.9 |
| CVE ID | CVE-2000-0234 | | |
| Vendor Reference: | - | | |
| Bugtraq ID | 1083 | | |
| Last Update: | 11/30/2005 | | |

THREAT:
.htaccess contains authentication information.

IMPACT:
Unauthorized users can gather authentication information from this file.

SOLUTION:

Change the Apache configuration so the .htaccess file cannot be accessed via the Internet.

RESULT:

```
##
# @version $Id: htaccess.txt 9795 2008-01-02 11:33:07Z rmuilwijk $
# @package Joomla
# @copyright Copyright (C) 2005 - 2008 Open Source Matters. All rights reserved.
# @license http://www.gnu.org/copyleft/gpl.html GNU/GPL
# Joomla! is Free Software
##

#####
# READ THIS COMPLETELY IF YOU CHOOSE TO USE THIS FILE
#
# The line just below this section: 'Options +FollowSymLinks' may cause problems
# with some server configurations. It is required for use of mod_rewrite, but may already
# be set by your server administrator in a way that disallows changing it in
# your .htaccess file. If using it causes your server to error out, comment it out (add # to
# beginning of line), reload your site in your browser and test your self url's. If they work,
# it has been set by your server administrator and you do not need it set here.
#
# Only use one of the two SEF sections that follow. Lines that can be uncommented
# (and thus used) have only one #. Lines with two #'s should not be uncommented
# In the section that you don't use, all lines should start with #
#
#####

## Can be commented out if causes errors, see notes above.
Options +FollowSymLinks

#
# mod_rewrite in use

RewriteEngine On

# Uncomment following line if your webserver's URL
# is not directly related to physical file paths.
# Update Your Joomla! Directory (just / for root)

# RewriteBase /

##### Begin - Joomla! core SEF Section
#
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteCond %{REQUEST_URI} !^/index.php
RewriteCond %{REQUEST_URI} (/\.php|\.html|\.htm|\.feed|\.pdf|\.raw|/[\^.]*)$ [NC]
RewriteRule (.*) index.php
RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization},L]
#
##### End - Joomla! core SEF Section

##### Begin - Rewrite rules to block out some common exploits
## If you experience problems on your site block out the operations listed below
## This attempts to block the most common type of exploit `attempts` to Joomla!
#
# Block out any script trying to set a mosConfig value through the URL
RewriteCond %{QUERY_STRING} mosConfig_[a-zA-Z_]{1,21}(=|\%3D) [OR]
# Block out any script trying to base64_encode crap to send via URL
RewriteCond %{QUERY_STRING} base64_encode.*(.*?) [OR]
# Block out any script that includes a <script> tag in URL
RewriteCond %{QUERY_STRING} (<|%)3C.*script.*(%)3E [NC,OR]
# Block out any script trying to set a PHP GLOBALS variable via URL
RewriteCond %{QUERY_STRING} GLOBALS(=|\\|%0-9A-Z){0,2} [OR]
# Block out any script trying to modify a _REQUEST variable via URL
RewriteCond %{QUERY_STRING} _REQUEST(=|\\|%0-9A-Z){0,2}
# Send all blocked request to homepage with 403 Forbidden error!
RewriteRule ^(.*)$ index.php [F,L]
#
##### End - Rewrite rules to block out some common exploits

# set the spam_ref variable
```

```

SetEnvIfNoCase Referer "musicforum.org.ua" spam_ref=1
SetEnvIfNoCase Referer "all-for-women.com" spam_ref=1
SetEnvIfNoCase Referer "detoxonline.org" spam_ref=1
SetEnvIfNoCase Referer "financereal.info" spam_ref=1
SetEnvIfNoCase Referer "health-db.com" spam_ref=1
SetEnvIfNoCase Referer "homes-db.com" spam_ref=1
SetEnvIfNoCase Referer "musicforum.org.ua" spam_ref=1
SetEnvIfNoCase Referer "all-for-women.com" spam_ref=1
SetEnvIfNoCase Referer "mp3clank.com" spam_ref=1
SetEnvIfNoCase Referer "music-db.org" spam_ref=1
SetEnvIfNoCase Referer "musicforum.org.ua" spam_ref=1
SetEnvIfNoCase Referer "1000000mp3.info" spam_ref=1
SetEnvIfNoCase Referer "newmusiccentre.co.uk" spam_ref=1
SetEnvIfNoCase Request_URI "postid=" spam_ref=1
# block all referres that have spam_ref set
<FilesMatch "(.*)">
Order Allow,Deny
Allow from all
Deny from env=spam_ref
</FilesMatch>

```

 3 Web Server Uses Plain-Text Form Based Authentication

port 80/tcp

```

QID: 86728 CVSS Base: 7
Category: Web server CVSS Temporal: 6.3
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 08/13/2007

```

PCI FAILED 

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.

RESULT:

```

GET /administrator/ HTTP/1.1
Host: ip-68-178-172-38.ip.secureserver.net
Connection: Keep-Alive

```

```

<form action="index.php" method="post" name="login" id="form-login" style="clear: both;">
<p id="form-login-username">
<label for="username">Username</label>
<input name="username" id="username" type="text" class="inputbox" size="15" />
</p>
<p id="form-login-password">
<label for="password">Password</label>
<input name="passwd" id="password" type="password" class="inputbox" size="15" />
</p>
<p id="form-login-lang" style="clear: both;">
<label for="lang">Language</label>
<select name="lang" id="lang" class="inputbox"><option value="" selected="selected">Default</option><option value="en-GB" >English (United Kingdom)</option></select> </p>
<div class="button_holder">
<div class="button1">
<div class="next">
<a onclick="login.submit();">
Login</a>
</div>

```

```
</div>
</div>
<div class="clr"></div>
<input type="submit" style="border: 0; padding: 0; margin: 0; width: 0px; height: 0px;" value="Login" />
<input type="hidden" name="option" value="com_login" />
<input type="hidden" name="task" value="login" />
<input type="hidden" name="b91fdcada80e4358f83213b364f539a" value="1" /></form>
```

2 TCP Sequence Number Approximation Based Denial of Service

| | | | |
|-------------------|-------------------------------|----------------|-----|
| QID: | 82054 | CVSS Base: | 3.3 |
| Category: | TCP/IP | CVSS Temporal: | 2.8 |
| CVE ID | CVE-2004-0230 | | |
| Vendor Reference: | - | | |
| Bugtraq ID | 10183 | | |
| Last Update: | 12/20/2007 | | |

THREAT:

TCP provides stateful communications between hosts on a network. TCP sessions are established by a three-way handshake and use random 32-bit sequence and acknowledgement numbers to ensure the validity of traffic. A vulnerability was reported that may permit TCP sequence numbers to be more easily approximated by remote attackers. This issue affects products released by multiple vendors.

The cause of the vulnerability is that affected implementations will accept TCP sequence numbers within a certain range, known as the acknowledgement range, of the expected sequence number for a packet in the session. This is determined by the TCP window size, which is negotiated during the three-way handshake for the session. Larger TCP window sizes may be set to allow for more throughput, but the larger the TCP window size, the more probable it is to guess a TCP sequence number that falls within an acceptable range. It was initially thought that guessing an acceptable sequence number was relatively difficult for most implementations given random distribution, making this type of attack impractical. However, some implementations may make it easier to successfully approximate an acceptable TCP sequence number, making these attacks possible with a number of protocols and implementations.

This is further compounded by the fact that some implementations may support the use of the TCP Window Scale Option, as described in RFC 1323, to extend the TCP window size to a maximum value of 1 billion.

This vulnerability will permit a remote attacker to inject a SYN or RST packet into the session, causing it to be reset and effectively allowing for denial of service attacks. An attacker would exploit this issue by sending a packet to a receiving implementation with an approximated sequence number and a forged source IP address and TCP port.

There are a few factors that may present viable target implementations, such as those which depend on long-lived TCP connections, those that have known or easily guessed IP address endpoints and those implementations with easily guessed TCP source ports. It has been noted that Border Gateway Protocol (BGP) is reported to be particularly vulnerable to this type of attack, due to the use of long-lived TCP sessions and the possibility that some implementations may use the TCP Window Scale Option. As a result, this issue is likely to affect a number of routing platforms.

Another factor to consider is the relative difficulty of injecting packets into TCP sessions, as a number of receiving implementations will reassemble packets in order, dropping any duplicates. This may make some implementations more resistant to attacks than others.

It should be noted that while a number of vendors have confirmed this issue in various products, investigations are ongoing and it is likely that many other vendors and products will turn out to be vulnerable as the issue is investigated further.

IMPACT:

Successful exploitation of this issue could lead to denial of service attacks on the TCP based services of target hosts. Other consequences may also result, such as man-in-the-middle attacks.

SOLUTION:

Please first check the results section below for the port number on which this vulnerability was detected. If that port number is known to be used for port-forwarding, then it is the backend host that is really vulnerable.

Various implementations and products including Check Point, Cisco, Cray Inc, Hitachi, Internet Initiative Japan, Inc (IJ), Juniper Networks, NEC, Polycm, and Yamaha are currently undergoing review. Contact the vendors to obtain more information about affected products and fixes. NISCC Advisory 236929 - Vulnerability Issues in TCP details the vendor patch status as of the time of the advisory, and identifies resolutions and workarounds.

The Internet Engineering Task Force (IETF) has developed an Internet-Draft titled Transmission Control Protocol Security Considerations that

addresses this issue.

Workaround:

The following BGP-specific workaround information has been provided.

For BGP implementations that support it, the TCP MD5 Signature Option should be enabled. Passwords that the MD5 checksum is applied to should be set to strong values and changed on a regular basis.

Secure BGP configuration instructions have been provided for Cisco and Juniper at these locations:

<http://www.cymru.com/Documents/secure-bgp-template.html>

<http://www.qorbit.net/documents/junos-bgp-template.pdf>

RESULT:

Tested on port 22 with an injected SYN/RST offset by 16 bytes.

Tested on port 25 with an injected SYN/RST offset by 16 bytes.



2 AutoComplete Attribute Not Disabled for Password in Form Based Authentication

port 80/tcp

| | | | |
|-------------------|------------|----------------|-----|
| QID: | 86729 | CVSS Base: | 3.5 |
| Category: | Web server | CVSS Temporal: | 3.3 |
| CVE ID: | - | | |
| Vendor Reference: | - | | |
| Bugtraq ID: | - | | |
| Last Update: | 01/12/2006 | | |

THREAT:

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

IMPACT:

The passwords entered by one user could be stored by the browser and retrieved for another user using the browser.

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.

RESULT:

GET /administrator/ HTTP/1.1

Host: ip-68-178-172-38.ip.secureserver.net

Connection: Keep-Alive

```
<form action="index.php" method="post" name="login" id="form-login" style="clear: both;">
<p id="form-login-username">
<label for="username">Username</label>
<input name="username" id="username" type="text" class="inputbox" size="15" />
</p>
```

```
<p id="form-login-password">
<label for="password">Password</label>
<input name="passwd" id="password" type="password" class="inputbox" size="15" />
</p>
```

```
<p id="form-login-lang" style="clear: both;">
```

```
<label for="lang">Language</label>
```

```
<select name="lang" id="lang" class="inputbox"><option value="" selected="selected">Default</option><option value="en-GB" >English (United Kingdom)</option></select> </p>
```

```
<div class="button_holder">
```

```
<div class="button1">
```

```
<div class="next">
```

```
<a onclick="login.submit();">
```

```
Login</a>
```

```

</div>
</div>
</div>
<div class="clr"></div>
<input type="submit" style="border: 0; padding: 0; margin: 0; width: 0px; height: 0px;" value="Login" />
<input type="hidden" name="option" value="com_login" />
<input type="hidden" name="task" value="login" />
<input type="hidden" name="b91fdcada80e4358f83213b364f539a" value="1" /></form>

```



2 Web Server HTTP Trace/Track Method Support Cross-Site Tracing Vulnerability

port 80/tcp

QID: 86473 CVSS Base: 2.8
 Category: Web server CVSS Temporal: 2.4
 CVE ID [CVE-2004-2320](#), [CVE-2007-3008](#)
 Vendor Reference: -
 Bugtraq ID: -
 Last Update: 12/04/2007

PCI FAILED

THREAT:

A Web server was detected that supports the HTTP TRACE method. This method allows debugging and connection trace analysis for connections from the client to the Web server. Per the HTTP specification, when this method is used, the Web server echoes back the information sent to it by the client unmodified and unfiltered. Microsoft IIS web server uses an alias TRACK for this method, and is functionally the same.

A vulnerability related to this method was discovered. A malicious, active component in a Web page can send Trace requests to a Web server that supports this Trace method. Usually, browser security disallows access to Web sites outside of the present site's domain. Although unlikely and difficult to achieve, it's possible, in the presence of other browser vulnerabilities, for the active HTML content to make external requests to arbitrary Web servers beyond the hosting Web server. Since the chosen Web server then echoes back the client request unfiltered, the response also includes cookie-based or Web-based (if logged on) authentication credentials that the browser automatically sent to the specified Web application on the specified Web server.

The significance of the Trace capability in this vulnerability is that the active component in the page visited by the victim user has no direct access to this authentication information, but gets it after the target Web server echoes it back as its Trace response.

Since this vulnerability exists as a support for a method required by the HTTP protocol specification, most common Web servers are vulnerable.

The exact method(s) supported, Trace and/or Track, and their responses are in the Results section below.

IMPACT:

If this vulnerability is successfully exploited, users of the Web server may lose their authentication credentials for the server and/or for the Web applications hosted by the server to an attacker. This may be the case even if the Web applications are not vulnerable to cross site scripting attacks due to input validation errors.

SOLUTION:

Solutions for some of the common Web servers are supplied below. For other Web servers, please check your vendor's documentation.

Apache: Recent Apache versions have a Rewrite module that allows HTTP requests to be rewritten or handled in a specific way. Compile the Apache server with the mod_rewrite module. You might need to uncomment the 'AddModule' and 'LoadModule' directives in the httpd.conf configuration file. Add the following lines for each virtualhost in your configuration file (Please note that, by default, Rewrite configurations are not inherited. This means that you need to have Rewrite directives for each virtual host in which you wish to use it):

```

<IfModule mod_rewrite.c>
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^TRACE
RewriteRule .* - [F]
</IfModule>

```

With this configuration, Apache catches all TRACE requests, and replies with a page reporting the request as forbidden. None of the original request's contents are echoed back.

A slightly tighter fix is to use:

```

<IfModule mod_rewrite.c>
RewriteEngine on
RewriteCond %{REQUEST_METHOD} !^(GET|POST|HEAD)$

```

```
RewriteRule .* - [F]
</IfModule>
```

Please note that RewriteEngine can be processor intensive and may impact the web server performance. The trace method can also be controlled by use of the TraceEnable directive, and track can be controlled through either the Limit or LimitExcept. In the httpd.conf add or modify:

```
<Directory>
<limit TRACK>
deny from all
</limit>
...
</Directory>
```

TraceEnable Off

Microsoft IIS: Microsoft released URLScan, which can be used to screen all incoming requests based on customized rulesets. URLScan can be used to sanitize or disable the TRACE requests from the clients. Note that IIS aliases 'TRACK' to 'TRACE'. Therefore, if URLScan is used to specifically block the TRACE method, the TRACK method should also be added to the filter.

URLScan uses the 'urlscan.ini' configuration file, usually in \System32\inetSrv\URLScan directory. In that, we have two sections - AllowVerbs and DenyVerbs. The former is used if the UseAllowVerbs variable is set to 1, else (if its set to 0), the DenyVerbs are used. Clearly, either can be used, depending on whether we want a Default-Deny-Explicit-Allow or a Default-Allow-Explicit-Deny policy. To disallow TRACE and TRACK methods through URLScan, first remove 'TRACK', 'TRACE' methods from the 'AllowVerbs' section and add them to the 'DenyVerbs' section. With this, URLScan will disallow all 'TRACE' and 'TRACK' methods, and generate an error page for all requests using that method. To enable the changes, restart the 'World Wide Web Publishing Service' from the 'Services' Control Panel item.

Sun ONE/iPlanet Web Server: Here are the sun recommendations to disable the trace method.

For more details about other web servers : Cert Advisory.

RESULT:

```
TRACE / HTTP/1.1
Host: ip-68-178-172-38.ip.secureserver.net
Via: <script>alert('QualysXSS');</script>
```

```
HTTP/1.1 200 OK
Date: Tue, 25 Mar 2008 23:58:18 GMT
Server: Apache/2.2.3 (CentOS)
Connection: close
Transfer-Encoding: chunked
Content-Type: message/http
```

```
TRACE / HTTP/1.1
Host: ip-68-178-172-38.ip.secureserver.net
Via: <script>alert('QualysXSS');</script>
```

```
-CR-TRACE / HTTP/1.0
Via: <script>alert('QualysXSS');</script>
```

```
HTTP/1.1 200 OK
Date: Tue, 25 Mar 2008 23:58:18 GMT
Server: Apache/2.2.3 (CentOS)
Connection: close
Content-Type: message/http
```

```
TRACE / HTTP/1.0
Via: <script>alert('QualysXSS');</script>
```



2 Web Directories Listable Vulnerability

port 80/tcp

| | | | |
|-----------|------------|----------------|-----|
| QID: | 86445 | CVSS Base: | 2.3 |
| Category: | Web server | CVSS Temporal: | 2.1 |
| CVE ID: | - | | |

Vendor Reference: -
Bugtraq ID: -
Last Update: 11/07/2005

THREAT:

The Web server has some listable directories. Very sensitive information can be obtained from directory listings.

IMPACT:

A remote user may exploit this vulnerability to obtain very sensitive information on the host. The information obtained may assist in further attacks against the host.

SOLUTION:

Disable directory browsing or listing for all directories.

RESULT:

Listable Directories
/src/

 2 SSL Certificate - Signature Verification Failed Vulnerability port 443/tcp over SSL

QID: 38173 CVSS Base: 3.7
Category: General remote services CVSS Temporal: 3.1
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 11/07/2005

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. The authentication is done by verifying that the public key in the certificate is signed by a trusted third-party Certificate Authority.

If a client is unable to verify the certificate, it can abort communication or prompt the user to continue the communication without authentication.

IMPACT:

By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.

Exception:

If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.

SOLUTION:

Please install a server certificate signed by a trusted third-party Certificate Authority.

RESULT:

Certificate #0 unable to get local issuer certificate

 2 Web Directories Listable Vulnerability port 443/tcp

QID: 86445 CVSS Base: 2.3
Category: Web server CVSS Temporal: 2.1
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 11/07/2005

THREAT:

The Web server has some listable directories. Very sensitive information can be obtained from directory listings.

IMPACT:

A remote user may exploit this vulnerability to obtain very sensitive information on the host. The information obtained may assist in further attacks against the host.

SOLUTION:

Disable directory browsing or listing for all directories.

RESULT:

Listable Directories

/src/



2 Web Server HTTP Trace/Track Method Support Cross-Site Tracing Vulnerability

port 443/tcp

| | | | |
|-------------------|---|----------------|-----|
| QID: | 86473 | CVSS Base: | 2.8 |
| Category: | Web server | CVSS Temporal: | 2.4 |
| CVE ID | CVE-2004-2320 , CVE-2007-3008 | | |
| Vendor Reference: | - | | |
| Bugtraq ID: | - | | |
| Last Update: | 12/04/2007 | | |

PCI FAILED

THREAT:

A Web server was detected that supports the HTTP TRACE method. This method allows debugging and connection trace analysis for connections from the client to the Web server. Per the HTTP specification, when this method is used, the Web server echoes back the information sent to it by the client unmodified and unfiltered. Microsoft IIS web server uses an alias TRACK for this method, and is functionally the same.

A vulnerability related to this method was discovered. A malicious, active component in a Web page can send Trace requests to a Web server that supports this Trace method. Usually, browser security disallows access to Web sites outside of the present site's domain. Although unlikely and difficult to achieve, it's possible, in the presence of other browser vulnerabilities, for the active HTML content to make external requests to arbitrary Web servers beyond the hosting Web server. Since the chosen Web server then echoes back the client request unfiltered, the response also includes cookie-based or Web-based (if logged on) authentication credentials that the browser automatically sent to the specified Web application on the specified Web server.

The significance of the Trace capability in this vulnerability is that the active component in the page visited by the victim user has no direct access to this authentication information, but gets it after the target Web server echoes it back as its Trace response.

Since this vulnerability exists as a support for a method required by the HTTP protocol specification, most common Web servers are vulnerable.

The exact method(s) supported, Trace and/or Track, and their responses are in the Results section below.

IMPACT:

If this vulnerability is successfully exploited, users of the Web server may lose their authentication credentials for the server and/or for the Web applications hosted by the server to an attacker. This may be the case even if the Web applications are not vulnerable to cross site scripting attacks due to input validation errors.

SOLUTION:

Solutions for some of the common Web servers are supplied below. For other Web servers, please check your vendor's documentation.

Apache: Recent Apache versions have a Rewrite module that allows HTTP requests to be rewritten or handled in a specific way. Compile the Apache server with the mod_rewrite module. You might need to uncomment the 'AddModule' and 'LoadModule' directives in the httpd.conf configuration file. Add the following lines for each virtualhost in your configuration file (Please note that, by default, Rewrite configurations are not inherited. This means that you need to have Rewrite directives for each virtual host in which you wish to use it):

```
<IfModule mod_rewrite.c>
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^TRACE
```

```
RewriteRule .* - [F]
</IfModule>
```

With this configuration, Apache catches all TRACE requests, and replies with a page reporting the request as forbidden. None of the original request's contents are echoed back.

A slightly tighter fix is to use:

```
<IfModule mod_rewrite.c>
RewriteEngine on
RewriteCond %{REQUEST_METHOD} !^(GET|POST|HEAD)$
RewriteRule .* - [F]
</IfModule>
```

Please note that RewriteEngine can be processor intensive and may impact the web server performance. The trace method can also be controlled by use of the TraceEnable directive, and track can be controlled through either the Limit or LimitExcept. In the httpd.conf add or modify:

```
<Directory>
<limit TRACE>
deny from all
</limit>
...
</Directory>
```

TraceEnable Off

Microsoft IIS: Microsoft released URLScan, which can be used to screen all incoming requests based on customized rulesets. URLScan can be used to sanitize or disable the TRACE requests from the clients. Note that IIS aliases 'TRACK' to 'TRACE'. Therefore, if URLScan is used to specifically block the TRACE method, the TRACK method should also be added to the filter.

URLScan uses the 'urlscan.ini' configuration file, usually in \System32\inetSrv\URLScan directory. In that, we have two sections - AllowVerbs and DenyVerbs. The former is used if the UseAllowVerbs variable is set to 1, else (if its set to 0), the DenyVerbs are used. Clearly, either can be used, depending on whether we want a Default-Deny-Explicit-Allow or a Default-Allow-Explicit-Deny policy. To disallow TRACE and TRACK methods through URLScan, first remove 'TRACK', 'TRACE' methods from the 'AllowVerbs' section and add them to the 'DenyVerbs' section. With this, URLScan will disallow all 'TRACE' and 'TRACK' methods, and generate an error page for all requests using that method. To enable the changes, restart the 'World Wide Web Publishing Service' from the 'Services' Control Panel item.

Sun ONE/iPlanet Web Server: Here are the sun recommendations to disable the trace method.

For more details about other web servers : Cert Advisory.

RESULT:

```
TRACE / HTTP/1.1
Host: ip-68-178-172-38.ip.secureserver.net
Via: <script>alert('QualysXSS');</script>
```

```
HTTP/1.1 200 OK
Date: Tue, 25 Mar 2008 23:52:58 GMT
Server: Apache/2.2.3 (CentOS)
Connection: close
Transfer-Encoding: chunked
Content-Type: message/http
```

```
TRACE / HTTP/1.1
Host: ip-68-178-172-38.ip.secureserver.net
Via: <script>alert('QualysXSS');</script>
```

```
-CR-TRACE / HTTP/1.0
Via: <script>alert('QualysXSS');</script>
```

```
HTTP/1.1 200 OK
Date: Tue, 25 Mar 2008 23:52:58 GMT
Server: Apache/2.2.3 (CentOS)
Connection: close
```

Content-Type: message/http

TRACE / HTTP/1.0

Via: <script>alert('QualysXSS');</script>



2 AutoComplete Attribute Not Disabled for Password in Form Based Authentication

port 443/tcp

| | | | |
|-------------------|------------|----------------|-----|
| QID: | 86729 | CVSS Base: | 3.5 |
| Category: | Web server | CVSS Temporal: | 3.3 |
| CVE ID: | - | | |
| Vendor Reference: | - | | |
| Bugtraq ID: | - | | |
| Last Update: | 01/12/2006 | | |

THREAT:

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

IMPACT:

The passwords entered by one user could be stored by the browser and retrieved for another user using the browser.

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.

RESULT:

GET /login/?user=|`id`| HTTP/1.1
Host: ip-68-178-172-38.ip.secureserver.net
Connection: Keep-Alive

```
<form action="/login" method="post" name="login" id="form-login">
<table width="100%" border="0" align="center" cellpadding="4" cellspacing="0" class="contentpane">
<tr>
<td colspan="2">
<div class="componentheading">
Login to ModPHP.org </div>
<div>
 </div>
</td>
</tr>
<tr>
<td colspan="2">
</td>
</tr>
</table>
<fieldset class="input">
<p id="form-login-username">
<label for="username">Username</label><br />
<input name="username" id="username" type="text" class="inputbox" alt="username" size="18" />
</p>
<p id="form-login-password">
<label for="passwd">Password</label><br />
<input type="password" name="passwd" class="inputbox" size="18" alt="password" />
</p>
<p id="form-login-remember">
<label for="remember">Remember Me</label>
<input type="checkbox" name="remember" class="inputbox" value="yes" alt="Remember Me" />
</p>
<input type="submit" name="Submit" class="button" value="Login" />
</fieldset>
<ul>
<li>
<a href="/login">
Forgot your Password?</a>
</li>
<li>
<a href="/login">
Forgot your Username?</a>
</li>
<li>
<a href="/login?task=register">
Register</a>
</li>
</ul>
```



```
<input type="hidden" name="option" value="com_user" />
<input type="hidden" name="task" value="login" />
<input type="hidden" name="return" value="" />
<input type="hidden" name="803ee80cdc9176e9ace37acbc803c7e" value="1" /></form>
```

Potential Vulnerabilities (2)

4 OpenSSH Signal Handling Vulnerability (RHSA-2006-0697)

QID: 38560 CVSS Base: 8
Category: General remote services CVSS Temporal: 5.9
CVE ID [CVE-2006-5051](#), [CVE-2006-4924](#)
Vendor Reference [RHSA-2006-0697](#)
Bugtraq ID: -
Last Update: 01/11/2008

PCI FAILED 

THREAT:

A vulnerability in OpenSSH is caused due to a race condition within the signal handling.

IMPACT:

This can be exploited to crash the OpenSSH server and potentially allows the execution of arbitrary code.

SOLUTION:

Red Hat has released security advisory 2006-0697 to address this issue.

A newer update RHBA-2007-0462 is available which obsoletes RHSA-2006-0697

RESULT:

SSH-2.0-OpenSSH_4.3

3 Possible Mail Relay

port 25/tcp

QID: 74037 CVSS Base: 7
Category: Mail services CVSS Temporal: 6.3
CVE ID [CVE-1999-0512](#), [CVE-2002-1278](#), [CVE-2003-0285](#)
Vendor Reference: -
Bugtraq ID: -
Last Update: 11/08/2005

PCI FAILED 

THREAT:

The Internet Electronic Mail exchange protocol (SMTP) is designed to work with relays. These days, there is less of a need for relaying functions and, in fact, relaying functions are highly vulnerable to attacks because they allow unauthorized users to connect once to a mail server for a single message. Then, the relaying server distributes the message to thousands of recipients.

It is possible that mail relaying is allowed by the mail server on the host. More details about the specific relaying addresses that are accepted by the mail server are given in the Results section. Since a mail server that accepts a relaying address may be configured not to actually deliver the mail to that address. If this is the case, you may safely ignore this report.

IMPACT:

If mail relaying is indeed allowed, unauthorized Internet users can exploit your Mail server to send anonymous e-mail messages, send massive advertisement messages to unwilling recipients, consume bandwidth or cause denial of service on your servers.

SOLUTION:

Disallow mail relaying if it is allowed. The mail exchanger will need to be reconfigured accordingly.

RESULT:

HELO qualysguard.com

250 ip-68-178-172-38.ip.secureserver.net

MAIL FROM:<qgmrfm@ip-68-178-172-38.ip.secureserver.net>

250 ok

RCPT TO:<@qualysguard.com;qgmrtest@ip-68-178-172-38.ip.secureserver.net>

250 ok

DATA

354 go ahead

QG mail relay test # 6

250 ok 1206488604 qp 16007

Information Gathered (11)

2 Host Uptime Based on TCP TimeStamp Option

QID: 82063
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 05/29/2007

THREAT:

The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.

Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

RESULT:

Based on TCP timestamps obtained via port 22, the host's uptime is 6 days, 13 hours, and 33 minutes. The TCP timestamps from the host are in units of 1 milliseconds.

2 Operating System Detected

QID: 45017
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 02/09/2005

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.

Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that for the firewall instead of for the host being scanned.

2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).

3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.

4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB-II.system.sysDescr" for the operating system.

| RESULT: | Technique | ID |
|------------------|--------------------|----------|
| Operating System | | |
| Linux 2.4-2.6 | TCP/IP Fingerprint | U1141:22 |

1 DNS Host Name

QID: 6
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 12/31/1997

THREAT:

The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

| RESULT: | Host name |
|---------------|--------------------------------------|
| IP address | |
| 68.178.172.38 | ip-68-178-172-38.ip.secureserver.net |

1 Traceroute


QID: 45006
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 05/09/2003

THREAT:

Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

| RESULT: | IP | Round Trip Time | Probe |
|---------|----|-----------------|-------|
| Hops | | | |

| | | | |
|----|-----------------|---------|------|
| 1 | 64.39.104.1 | 0.45ms | ICMP |
| 2 | 38.119.54.129 | 0.25ms | ICMP |
| 3 | 38.112.37.193 | 0.39ms | ICMP |
| 4 | 66.28.4.182 | 5.65ms | ICMP |
| 5 | 154.54.1.34 | 1.29ms | ICMP |
| 6 | 154.54.6.190 | 1.57ms | ICMP |
| 7 | 64.215.195.153 | 19.07ms | ICMP |
| 8 | 64.210.13.110 | 11.09ms | ICMP |
| 9 | 208.109.112.198 | 11.42ms | ICMP |
| 10 | 208.109.112.129 | 11.40ms | ICMP |
| 11 | 216.69.188.14 | 11.38ms | ICMP |
| 12 | 68.178.169.243 | 11.45ms | TCP |
| 13 | 68.178.172.38 | 38.00ms | ICMP |

 1 Open TCP Services List

QID: 82023
 Category: TCP/IP
 CVE ID: -
 Vendor Reference: -
 Bugtraq ID: -
 Last Update: -

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.

RESULT:

| Port | IANA Assigned Ports/Services | Description | Service Detected | OS On Redirected Port |
|------|------------------------------|----------------------------|------------------|-----------------------|
| 80 | www | World Wide Web HTTP | http | |
| 443 | https | http protocol over TLS/SSL | http over ssl | |
| 22 | ssh | SSH Remote Login Protocol | ssh | |
| 25 | smtp | Simple Mail Transfer | smtp | |
| 3306 | mysql | MySQL | mysql | |

 1 SSL Web Server Version

port 443/tcp

QID: 86001
 Category: Web server
 CVE ID: -
 Vendor Reference: -
 Bugtraq ID: -
 Last Update: -

RESULT:

| Server Version | Server Banner |
|----------------|-----------------------|
| Apache 1.3 | Apache/2.2.3 (CentOS) |

1 Web Server Version

port 80/tcp

QID: 86000
Category: Web server
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 12/31/1997

Table with 2 columns: Server Version, Server Banner. Row 1: Apache 1.3, Apache/2.2.3 (CentOS)

1 Open UDP Services List

QID: 82004
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 07/11/2005

THREAT:
A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.

Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host.

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team.

Table with 4 columns: Port, IANA Assigned Ports/Services, Description, Service Detected. Rows include ports 69, 138, 161, 135, 137, 53.

1 Firewall Detected


QID: 34011
Category: Firewall
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 10/16/2001

THREAT:

A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

RESULT:

Some of the ports filtered by the firewall are: 135, 139, 1028, 1080, 3128, 8080.

 1 Host Names Found

QID: 45039
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 02/14/2005

THREAT:

The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

RESULT:

| Host Name | Source |
|--------------------------------------|--------|
| ip-68-178-172-38.ip.secureserver.net | FQDN |

 1 Host Scan Time

QID: 45038
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 11/19/2004

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

RESULT:

Scan duration: 1851 seconds

Start time: Tue, Mar 25 2008, 23:39:34 GMT

End time: Wed, Mar 26 2008, 00:10:25 GMT

Appendices

Hosts Scanned

68.178.172.38

Option Profile

Scan

| | |
|---|---------------|
| Scanned TCP Ports: | Full |
| Scanned UDP Ports: | Standard Scan |
| Scan Dead Hosts: | Off |
| Load Balancer Detection: | Off |
| Password Brute Forcing: | Standard |
| Vulnerability Detection: | Complete |
| Windows Authentication: | Disabled |
| SSH Authentication: | Disabled |
| Oracle Authentication: | Disabled |
| SNMP Authentication: | Disabled |
| Perform 3-way Handshake: | Off |
| Overall Performance: | Custom |
| Hosts to Scan in Parallel-External Scanner: | 15 |
| Hosts to Scan in Parallel-Scanner Appliances: | 15 |
| Processes to Run in Parallel-Total: | 10 |
| Processes to Run in Parallel-HTTP: | 10 |
| Packet (Burst) Delay: | Medium |

Advanced

| | |
|---|---|
| Hosts Discovery: | TCP Standard Scan, UDP Standard Scan, ICMP On |
| Ignore RST packets: | Off |
| Ignore firewall-generated SYN-ACK packets: | Off |
| Do not send ACK or SYN-ACK packets during host discovery: | Off |

Report Legend

Payment Card Industry (PCI) Status

The Detailed Results section of the report shows all detected vulnerabilities and potential vulnerabilities sorted by host. The vulnerabilities and potential vulnerabilities marked PCI FAILED caused the host to receive the PCI compliance status FAILED. All vulnerabilities and potential vulnerabilities marked PCI FAILED must be remediated to pass the PCI compliance requirements. Vulnerabilities not marked as PCI FAILED display vulnerabilities that the PCI Compliance service found on the hosts when scanned. Although these vulnerabilities are not in scope for PCI, we do recommend that you remediate the vulnerabilities in severity order.






A PCI compliance status of PASSED for a single host/IP indicates that no vulnerabilities or potential vulnerabilities, as defined by the PCI DSS compliance standards set by the PCI Council, were detected on the host. An overall PCI compliance status of PASSED indicates that all hosts in the report passed the PCI compliance standards.

A PCI compliance status of FAILED for a single host/IP indicates that at least one vulnerability or potential vulnerability, as defined by the PCI DSS compliance standards set by the PCI Council, was detected on the host. An overall PCI compliance status of FAILED indicates that at least one host in the report failed to meet the PCI compliance standards.

Vulnerability Levels






A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

| Severity | Level | Description |
|----------|-------|-------------|
|----------|-------|-------------|

| | | | |
|---|---|----------|---|
|  | 1 | Minimal | Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities. |
|  | 2 | Medium | Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions. |
|  | 3 | Serious | Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying. |
|  | 4 | Critical | Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host. |
|  | 5 | Urgent | Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors. |




Potential Vulnerability Levels

A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.

| Severity | Level | Description | |
|---|-------|-------------|--|
|  | 1 | Minimal | If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities. |
|  | 2 | Medium | If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions. |
|  | 3 | Serious | If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying. |
|  | 4 | Critical | If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host. |
|  | 5 | Urgent | If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors. |

Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

| Severity | Level | Description | |
|---|-------|-------------|---|
|  | 1 | Minimal | Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls. |
|  | 2 | Medium | Intruders may be able to determine the operating system running on the host, and view banner versions. |
|  | 3 | Serious | Intruders may be able to detect highly sensitive data, such as global system user lists. |