QUALYS FREESCAN

Vulnerability Scan

06 July 2015 at 13:00

URL : https://fdago.conceptplusllc.net

Summary: 20 vulnerabilities found

HIGH 0 MED 8 LOW 12 INFO 28

Name	Vulnerability
Slow HTTP headers vulnerability	
Directory Listing	
Directory Listing	
Cookie Does Not Contain The "HTTPOnly" Attribute	
Cookie Does Not Contain The "secure" Attribute	
Listing of Scripts in the scripts Directory	
Listing of Scripts in the scripts Directory	
Apache Prior to 2.4.4 and 2.2.24 Multiple Vulnerabilities	
Apache HTTP Server Prior to 2.2.25 Multiple Vulnerabilities	
Apache HTTP Server Prior to 2.2.23 Multiple Vulnerabilities	
Apache Prior to 2.4.4 and 2.2.24 Multiple Vulnerabilities	
Apache HTTP Server Prior to 2.2.25 Multiple Vulnerabilities	
SSL Certificate - Subject Common Name Does Not Match Server FQDN	
Web Server Internal IP Address/Internal Network Name Disclosure Vulnerability	
Web Directories Listable Vulnerability	
Web Server Internal IP Address/Internal Network Name Disclosure Vulnerability	
SSL Certificate - Signature Verification Failed Vulnerability	

	Web Directories Listable Vulnerability	
	Apache Web Server ETag Header Information Disclosure Weakness	
	Apache Web Server ETag Header Information Disclosure Weakness	
	Server accepts unnecessarily large POST request body	INFO
	DEFLATE Data Compression Algorithm Used for HTTPS	INFO
	Web Server Probed For Various URL-Encoding Schemes Supported	INFO
	Web Server Probed For Various URL-Encoding Schemes Supported	INFO
	Firewall Detected	INFO
	Open TCP Services List	INFO
	SSL Web Server Version	INFO
	Web Server Version	INFO
	Internet Service Provider	INFO
	Default Web Page	INFO
	TLS Secure Renegotiation Extension Supported	INFO
	SSL Session Caching Information	INFO
	SSL Certificate - Information	INFO
	Host Names Found	INFO
	SSL/TLS invalid protocol version tolerance	INFO
	SSL/TLS Server supports TLS_FALLBACK_SCSV	INFO
	Degree of Randomness of TCP Initial Sequence Numbers	INFO
	List of Web Directories	INFO
	DNS Host Name	INFO
	SSL Server Information Retrieval	INFO
	Host Scan Time	INFO
	IP ID Values Randomness	INFO

	Default Web Page	INFO
	HTTP Methods Returned by OPTIONS Request	INFO
	List of Web Directories	INFO
	Target Network Information	INFO
	Traceroute	INFO
	HTTP Methods Returned by OPTIONS Request	INFO

Detailed results

Type: **Web Application**

Slow HTTP headers vulnerability

QID: 150079 **CVSS Base: 6.8**
Category: Web Application **Port: -**
CVEID: -

Threat:
The web application is possibly vulnerable to "slow HTTP headers" Denial of Service (DoS) attack. This is an application-level DoS, that occurs when an attacker holds server connections open by sending partial HTTP requests, and continues to send subsequent headers at some interval to prevent the server from closing sockets. In this way, the web server becomes unavailable because the number of available sockets decreases and memory usage may increase, especially if the server allocates a thread per connection. One of the reasons for this behavior is that some servers have "no data" timers, that reset each time a byte arrives at the socket, but the server does not enforce an overall time limit for a connection. For example, the attacker sends the data for its request one byte at a time over several minutes rather than following the expected behavior of transmitting a complete request of several hundred bytes in a single packet. This enables the attacker to prolong the connection virtually forever. More information can be found at the Slowloris HTTP DoS .

Impact:
All other services remain intact but the web server itself becomes completely inaccessible.

Solution:
Server-specific recommendations can be found here . Countermeasures for Apache are described here . Easy to use tool for intrusive testing is available here .

Results:
```
https://fdago.conceptplusllc.net/ -- Vulnerable to slow HTTP headers
attack Server resets timeout after accepting header data from peer.
```

Directory Listing

QID: 150023 **CVSS Base: 5**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
https://fdago.conceptplusllc.net/views/. -- <head> <title>Index of
/views</title> </head> <body> <h1>Index of /views</h1> <table><tr>
<th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?
C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th>
<th><a href="?C=S;O=A">Size</a></th><th><a href="?
C=D;O=A">Description</a></th></tr><tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[DIR]"></td>
<td><a href="/">Parent Directory</a></td><td> </td><td
align="right">  - </td><td>&nbs
```

Directory Listing

QID: 150023 **CVSS Base: 5**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
https://fdago.conceptplusllc.net/images/. -- <head> <title>Index of
/images</title> </head> <body> <h1>Index of /images</h1> <table><tr>
<th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?
C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th>
<th><a href="?C=S;O=A">Size</a></th><th><a href="?
C=D;O=A">Description</a></th></tr><tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[DIR]"></td>
<td><a href="/">Parent Directory</a></td><td> </td><td
align="right">  - </td><td>&nbs
```

Cookie Does Not Contain The "HTTPOnly" Attribute

QID: 150123 **CVSS Base:**
Category: Web Application **Port: -**
CVEID: -

Threat:
The cookie does not contain the "HTTPOnly" attribute.

Impact:
Cookies without the "HTTPOnly" attribute are permitted to be accessed via JavaScript.

Cross-site scripting attacks can steal cookies which could lead to user impersonation or compromise of the application account.

Solution:
If the associated risk of a compromised account is high, apply the "HTTPOnly" attribute to cookies.

Results:
```
https://fdago.conceptplusllc.net/ --
_ga=GA1.3.1506366539.1436200648; expires=Wed Jul 5 09:37:27 2017;
path=/; domain=fdago.conceptplusllc.net; max-age=63071935
```

Cookie Does Not Contain The "secure" Attribute

QID: 150122 **CVSS Base:**
Category: Web Application **Port: -**
CVEID: -

Threat:
The cookie does not contain the "secure" attribute.

Impact:
Cookies with the "secure" attribute are only permitted to be sent via HTTPS. Session cookies sent via HTTP expose an unsuspecting user to sniffing attacks that could lead to user impersonation or compromise of the application account.

Solution:
If the associated risk of a compromised account is high, apply the "secure" attribute to cookies and force all sensitive requests to be sent via HTTPS.

Results:
```
https://fdago.conceptplusllc.net/ -- _gat=1; expires=Mon Jul 6
09:47:27 2015; path=/; domain=fdago.conceptplusllc.net; max-age=535
```

Type: **Vulnerability**

Listing of Scripts in the scripts Directory

QID: 86333 **CVSS Base: 3.3**
Category: Web server **Port: 443**
CVEID: -

Threat:
The listing of files in your scripts directory is allowed.

Impact:
By browsing the scripts directory, unauthorized users can obtain a list of the CGI scripts present on your server. With this information, they can implement further attacks on vulnerable CGI scripts.

Solution:
Set a more restrictive rule on your server to prevent directory listing of the scripts directory.

Results:
```
HTTP/1.1 200 OK Content-Type: text/html;charset=UTF-8 Date: Mon, 06
Jul 2015 16:44:07 GMT Server: Apache/2.2.22 (Ubuntu) Vary: Accept-
Encoding Content-Length: 1615 Connection: keep-alive <!DOCTYPE HTML
PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"> <html> <head> <title>Index
of /scripts</title> </head> <body> <h1>Index of /scripts</h1>
<table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a
```

```
href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last
modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?
C=D;O=A">Description</a></th></tr><tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[DIR]"></td>
<td><a href="/">Parent Directory</a></td><td> </td><td
align="right">  - </td><td> </td></tr> <tr><td valign="top"><img
src="/icons/unknown.gif" alt="[ ]"></td><td><a
href="scripts.4f5b0cd0.js">scripts.4f5b0cd0.js</a></td><td
align="right">05-Jul-2015 21:34 </td><td align="right">9.8K</td>
<td> </td></tr> <tr><td valign="top"><img src="/icons/unknown.gif"
alt="[ ]"></td><td><a
href="scripts.ab0b9379.js">scripts.ab0b9379.js</a></td><td
align="right">05-Jul-2015 21:42 </td><td align="right">536 </td>
<td> </td></tr> <tr><td valign="top"><img src="/icons/unknown.gif"
alt="[ ]"></td><td><a
href="vendor.0574ddc3.js">vendor.0574ddc3.js</a></td><td
align="right">05-Jul-2015 21:34 </td><td align="right">676K</td>
<td> </td></tr> <tr><td valign="top"><img src="/icons/unknown.gif"
alt="[ ]"></td><td><a
href="vendor.a2796c52.js">vendor.a2796c52.js</a></td><td
align="right">05-Jul-2015 21:42 </td><td align="right">564K</td>
<td> </td></tr> <tr><th colspan="5"><hr></th></tr> </table>
<address>Apache/2.2.22 (Ubuntu) Server at ec2-54-164-73-28.compute-
1.amazonaws.com Port 80</address> </body></html>
```


Listing of Scripts in the scripts Directory

QID: 86333 **CVSS Base: 3.3**
Category: Web server **Port: 80**
CVEID: -

Threat:
The listing of files in your scripts directory is allowed.

Impact:
By browsing the scripts directory, unauthorized users can obtain a list of the CGI scripts present on your server. With this information, they can implement further attacks on vulnerable CGI scripts.

Solution:
Set a more restrictive rule on your server to prevent directory listing of the scripts directory.

Results:

```
HTTP/1.1 200 OK Content-Type: text/html;charset=UTF-8 Date: Mon, 06
Jul 2015 16:41:44 GMT Server: Apache/2.2.22 (Ubuntu) Vary: Accept-
Encoding Content-Length: 1615 Connection: keep-alive <!DOCTYPE HTML
PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"> <html> <head> <title>Index
of /scripts</title> </head> <body> <h1>Index of /scripts</h1>
<table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a
href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last
modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?
C=D;O=A">Description</a></th></tr><tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[DIR]"></td>
<td><a href="/">Parent Directory</a></td><td> </td><td
align="right">  - </td><td> </td></tr> <tr><td valign="top"><img
src="/icons/unknown.gif" alt="[ ]"></td><td><a
href="scripts.4f5b0cd0.js">scripts.4f5b0cd0.js</a></td><td
align="right">05-Jul-2015 21:34 </td><td align="right">9.8K</td>
<td> </td></tr> <tr><td valign="top"><img src="/icons/unknown.gif"
alt="[ ]"></td><td><a
href="scripts.ab0b9379.js">scripts.ab0b9379.js</a></td><td
align="right">05-Jul-2015 21:42 </td><td align="right">536 </td>
<td> </td></tr> <tr><td valign="top"><img src="/icons/unknown.gif"
```

```
alt="[ ]"></td><td><a
href="vendor.0574ddc3.js">vendor.0574ddc3.js</a></td><td
align="right">05-Jul-2015 21:34 </td><td align="right">676K</td>
<td> </td></tr> <tr><td valign="top"><img src="/icons/unknown.gif"
alt="[ ]"></td><td><a
href="vendor.a2796c52.js">vendor.a2796c52.js</a></td><td
align="right">05-Jul-2015 21:42 </td><td align="right">564K</td>
<td> </td></tr> <tr><th colspan="5"><hr></th></tr> </table>
<address>Apache/2.2.22 (Ubuntu) Server at ec2-54-164-73-28.compute-
1.amazonaws.com Port 80</address> </body></html>
```

Apache Prior to 2.4.4 and 2.2.24 Multiple Vulnerabilities

QID: 87156 **CVSS Base: 4.3**
Category: Web server **Port: 443**
CVEID: CVE-2012-3499, CVE-2012-4558

Threat:
Apache HTTP Server is an HTTP web server application.
Apache HTTP Server is prone to multiple cross-site scripting vulnerabilities because it fails to properly sanitize user-supplied input.
- Various XSS flaws exist due to unescaped hostnames and URIs HTML output in mod_info, mod_status, mod_imagemap, mod_ldap, and mod_proxy_ftp.
- A XSS flaw affects the mod_proxy_balancer manager interface.
Affected Versions:
Apache HTTP Server prior to 2.4.4
Apache HTTP Server prior to 2.2.24

Impact:
An attacker may leverage these issues to execute arbitrary HTML and script code in the browser of an unsuspecting user in the context of the affected site. This may let the attacker launch additional attacks.

Solution:
These vulnerabilities have been patched in Apache 2.2.24 and 2.4.4. Refer to Apache httpd 2.4.4 Changelog and Apache httpd 2.2.24 Changelog .
Ubuntu users refer to Ubuntu advisory USN-1765-1 for affected packages and patching details, or update with your package manager.

Results:
```
QID 87156 detected on port 443 - Apache/2.2.22 (Ubuntu)
```

Apache HTTP Server Prior to 2.2.25 Multiple Vulnerabilities

QID: 87233 **CVSS Base: 4.3**
Category: Web server **Port: 80**
CVEID: CVE-2013-1896, CVE-2013-1862

Threat:
Apache HTTP Server is an HTTP web server application.
Apache HTTP Server versons before to 2.2.25 are exposed to following vulnerabilities:
mod_rewrite.c in the mod_rewrite module in the Apache HTTP Server 2.2.x before 2.2.25 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to execute arbitrary commands via an HTTP request containing an escape sequence for a terminal emulator (CVE-2013-1862).
mod_dav.c in the Apache HTTP Server versions before 2.2.25 do not properly determine whether DAV is enabled for a URI, which allows remote attackers to cause a denial of service (segmentation fault) via a MERGE request in which the URI is configured for handling by the mod_dav_svn module, but a certain href attribute in XML data refers to a non-DAV URI (CVE-2013-1896).

Impact:
Successfully exploiting these vulnerabilities might allow a remote attacker to execute code or cause denial of service.

Solution:
These vulnerabilities have been patched in Apache 2.2.25. Refer to Apache httpd 2.2.25 Changelog .

Results:
```
QID 87233 detected on port 80 - Apache/2.2.22 (Ubuntu)
```

Apache HTTP Server Prior to 2.2.23 Multiple Vulnerabilities

QID: 87133 **CVSS Base: 6.9**
Category: Web server **Port: 0**
CVEID: CVE-2012-2687, CVE-2012-0883

Threat:
Apache HTTP Server is an HTTP web server application.
Apache server prior to version 2.2.23 is affected by multiple issues:
Insecure LD_LIBRARY_PATH handling
Cross-site scripting in mod_negotiation when untrusted uploads are supported Affected Versions:
Apache HTTP Server prior to version 2.2.23

Impact:
Successful exploitation may lead to execution of arbitrary code on the system within the context of the affected applications.

Solution:
These vulnerabilities have been patched in Apache 2.2.23. Refer to Apache httpd 2.2 Security Vulnerabilities .

Results:
```
QID 87133 detected on port 80 - Apache/2.2.22 (Ubuntu)QID 87133
detected on port 443 - Apache/2.2.22 (Ubuntu)
```

Apache Prior to 2.4.4 and 2.2.24 Multiple Vulnerabilities

QID: 87156 **CVSS Base: 4.3**
Category: Web server **Port: 80**
CVEID: CVE-2012-3499, CVE-2012-4558

Threat:
Apache HTTP Server is an HTTP web server application.
Apache HTTP Server is prone to multiple cross-site scripting vulnerabilities because it fails to properly sanitize user-supplied input.
- Various XSS flaws exist due to unescaped hostnames and URIs HTML output in mod_info, mod_status, mod_imagemap, mod_ldap, and mod_proxy_ftp.
- A XSS flaw affects the mod_proxy_balancer manager interface.
Affected Versions:
Apache HTTP Server prior to 2.4.4
Apache HTTP Server prior to 2.2.24

Impact:
An attacker may leverage these issues to execute arbitrary HTML and script code in the browser of an unsuspecting user in the context of the affected site. This may let the attacker launch additional attacks.

Solution:
These vulnerabilities have been patched in Apache 2.2.24 and 2.4.4. Refer to Apache httpd

2.4.4 Changelog and Apache httpd 2.2.24 Changelog .
Ubuntu users refer to Ubuntu advisory USN-1765-1 for affected packages and patching details, or update with your package manager.

Results:
QID 87156 detected on port 80 - Apache/2.2.22 (Ubuntu)

Apache HTTP Server Prior to 2.2.25 Multiple Vulnerabilities

QID: 87233 **CVSS Base: 4.3**
Category: Web server **Port: 443**
CVEID: CVE-2013-1896, CVE-2013-1862

Threat:
Apache HTTP Server is an HTTP web server application.
Apache HTTP Server versons before to 2.2.25 are exposed to following vulnerabilities:
mod_rewrite.c in the mod_rewrite module in the Apache HTTP Server 2.2.x before 2.2.25 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to execute arbitrary commands via an HTTP request containing an escape sequence for a terminal emulator (CVE-2013-1862).
mod_dav.c in the Apache HTTP Server versions before 2.2.25 do not properly determine whether DAV is enabled for a URI, which allows remote attackers to cause a denial of service (segmentation fault) via a MERGE request in which the URI is configured for handling by the mod_dav_svn module, but a certain href attribute in XML data refers to a non-DAV URI (CVE-2013-1896).

Impact:
Successfully exploiting these vulnerabilities might allow a remote attacker to execute code or cause denial of service.

Solution:
These vulnerabilities have been patched in Apache 2.2.25. Refer to Apache httpd 2.2.25 Changelog .

Results:
QID 87233 detected on port 443 - Apache/2.2.22 (Ubuntu)

Type: **Vulnerability**

SSL Certificate - Subject Common Name Does Not Match Server FQDN

QID: 38170 **CVSS Base: 2.6**
Category: General remote services **Port: 443**
CVEID: -

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=*.conceptplusllc.net,OU=Domain_Control_Validated
(*.conceptplusllc.net) doesn't resolve (conceptplusllc.net) and IP
(54.164.73.28) don't match (*.conceptplusllc.net) doesn't resolve
```

Type: **Vulnerability**

Web Server Internal IP Address/Internal Network Name Disclosure Vulnerability

QID: 86247 **CVSS Base: 3.5**
Category: Web server **Port: 443**
CVEID: CVE-2000-0649

Threat:
Some Web servers contain a vulnerability giving remote attackers the ability to attain your internal IP address or internal network name.
An attacker connected to a host on your network using HTTPS (typically on port 443) could craft a specially formed GET request from the Web server resulting in a 3XX Object Moved error message containing the internal IP address or internal network name of the Web server.
A target host using HTTP may also be vulnerable to this issue.

Impact:
Successful exploitation of this vulnerability results in the disclosure of your internal IP address or internal network name, which could then be used in further attacks against the target host.

Solution:
There are no patches available at this time. Please contact your vendor for updates.
Workaround:
For IIS Web Server 6.x and prior:
Check the Microsoft article on how to set the Hostname instead of internal IP address for IIS.
For IIS 7.0
The release version of IIS7 by default includes the functionality of masking the IP address.
Refer to Removing an IIS server's IP address from HTTP responses.
For Apache Web Server:
Modify the Apache configuration file as follows:
- Set "ServerName" to a proper FQDN.
or
- Use module mod_rewrite to modify the 3xx error message returned by the server.
No workaround information is available for other Web servers at this time. Refer to your vendor for an appropriate workaround.

Results:
```
10.10.170.28
```

Web Directories Listable Vulnerability

QID: 86445 **CVSS Base: 2.3**
Category: Web server **Port: 80**

CVEID: -

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.

Results:
```
#table cols="1" Listable_Directories /scripts/ /images/
```

Web Server Internal IP Address/Internal Network Name Disclosure Vulnerability

QID: 86247 **CVSS Base: 3.5**
Category: Web server **Port: 80**
CVEID: CVE-2000-0649

Threat:
Some Web servers contain a vulnerability giving remote attackers the ability to attain your internal IP address or internal network name.
An attacker connected to a host on your network using HTTPS (typically on port 443) could craft a specially formed GET request from the Web server resulting in a 3XX Object Moved error message containing the internal IP address or internal network name of the Web server.
A target host using HTTP may also be vulnerable to this issue.

Impact:
Successful exploitation of this vulnerability results in the disclosure of your internal IP address or internal network name, which could then be used in further attacks against the target host.

Solution:
There are no patches available at this time. Please contact your vendor for updates.
Workaround:
For IIS Web Server 6.x and prior:
Check the Microsoft article on how to set the Hostname instead of internal IP address for IIS.
For IIS 7.0
The release version of IIS7 by default includes the functionality of masking the IP address.
Refer to Removing an IIS server's IP address from HTTP responses.
For Apache Web Server:
Modify the Apache configuration file as follows:
- Set "ServerName" to a proper FQDN.
or
- Use module mod_rewrite to modify the 3xx error message returned by the server.
No workaround information is available for other Web servers at this time. Refer to your vendor for an appropriate workaround.

Results:
```
10.10.170.28
```

Type: **Vulnerability**

SSL Certificate - Signature Verification Failed Vulnerability

QID: 38173 **CVSS Base: 3.7**
Category: General remote services **Port: 443**
CVEID: -

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.

Results:
```
Certificate #0 CN=*.conceptplusllc.net,OU=Domain_Control_Validated
unable to get local issuer certificate
```

Type: **Vulnerability**

Web Directories Listable Vulnerability

QID: 86445 **CVSS Base: 2.3**
Category: Web server **Port: 443**
CVEID: -

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.

Results:
```
#table cols="1" Listable_Directories /scripts/ /images/
```

Apache Web Server ETag Header Information Disclosure Weakness

QID: 86477 **CVSS Base: 2.3**
Category: Web server **Port: 443**
CVEID: CVE-2003-1418

Threat:
The Apache HTTP Server is a popular, open-source HTTP server for multiple platforms, including Windows, Unix, and Linux.

A cache management feature for Apache makes use of an entity tag (ETag) header. When this option is enabled and a request is made for a document relating to a file, an ETag response header is returned containing various file attributes for caching purposes. ETag information allows subsequent file requests to contain specific information, such as the file's inode number.
A weakness has been found in the generation of ETag headers under certain configurations implementing the FileETag directive. Among the file attributes included in the header is the file inode number that is returned to a client.

Affected Versions:
By default, all Versions of Apache are vulnerable.
In Apache Versions 1.3.22 and earlier, it's not possible to disable inodes in in ETag headers to mitigate this vulnerability, so Apache Version 1.3.22 and earlier are vulnerable at all times.
Apache Version 1.3.23 and later have a setting that can be modified to remove the inode info from the ETag Headers to mitigate this vulnerability. Apache Versions >= 1.3.23 allow the user to configure what goes into ETag. However, if the user does not configure Apache to not include inode in ETag, the Web server can still be vulnerable even if Apache >= 1.3.23 is being used.

Impact:
This vulnerability poses a security risk, as the disclosure of inode information may aid in launching attacks against other network-based services. For instance, NFS uses inode numbers to generate file handles.

Solution:
Workaround:
For Apache 1.3.22 and earlier:
There is no patch or remediation available for Apache Versions 1.3.22 and earlier since it's not possible to disable inodes in in ETag headers. Customers running versions of Apache <= 1.3.22 will need to upgrade to a later version and then apply the settings listed below (see Apache Version 1.3.23 and later), as versions of Apache 1.3.22 and earlier do not have the ability to configure these setting.
For Apache 1.3.23 and later: In Apache Version 1.3.23 and later, it's possible to configure the FileETag directive to generate ETag headers without inode information, which mitigates this vulnerability.
To do so, include "FileETag -INode" in the Apache server configuration file for a specific subdirectory.
In order to fix this vulnerability globally, for the Web server, use the option "FileETag None".
Use the option "FileETag MTime Size" if you just want to remove the Inode information.
OpenBSD:
OpenBSD has released a patch that fixes this vulnerability. After installing the patch, inode numbers returned from the server are encoded using a private hash to avoid the release of sensitive information.

Results:
22145-7dc-51a27a9100780

Apache Web Server ETag Header Information Disclosure Weakness

QID: 86477 **CVSS Base: 2.3**
Category: Web server **Port: 80**
CVEID: CVE-2003-1418

Threat:
The Apache HTTP Server is a popular, open-source HTTP server for multiple platforms, including Windows, Unix, and Linux.
A cache management feature for Apache makes use of an entity tag (ETag) header. When this option is enabled and a request is made for a document relating to a file, an ETag response header is returned containing various file attributes for caching purposes. ETag information allows subsequent file requests to contain specific information, such as the file's inode number.
A weakness has been found in the generation of ETag headers under certain configurations implementing the FileETag directive. Among the file attributes included in the header is the

file inode number that is returned to a client.

Affected Versions:

By default, all Versions of Apache are vulnerable.
In Apache Versions 1.3.22 and earlier, it's not possible to disable inodes in in ETag headers to mitigate this vulnerability, so Apache Version 1.3.22 and earlier are vulnerable at all times.
Apache Version 1.3.23 and later have a setting that can be modified to remove the inode info from the ETag Headers to mitigate this vulnerability. Apache Versions >= 1.3.23 allow the user to configure what goes into ETag. However, if the user does not configure Apache to not include inode in ETag, the Web server can still be vulnerable even if Apache >= 1.3.23 is being used.

Impact:

This vulnerability poses a security risk, as the disclosure of inode information may aid in launching attacks against other network-based services. For instance, NFS uses inode numbers to generate file handles.

Solution:

Workaround:

For Apache 1.3.22 and earlier:

There is no patch or remediation available for Apache Versions 1.3.22 and earlier since it's not possible to disable inodes in in ETag headers. Customers running versions of Apache <= 1.3.22 will need to upgrade to a later version and then apply the settings listed below (see Apache Version 1.3.23 and later), as versions of Apache 1.3.22 and earlier do not have the ability to configure these setting.

For Apache 1.3.23 and later: In Apache Version 1.3.23 and later, it's possible to configure the FileETag directive to generate ETag headers without inode information, which mitigates this vulnerability.
To do so, include "FileETag -INode" in the Apache server configuration file for a specific subdirectory.
In order to fix this vulnerability globally, for the Web server, use the option "FileETag None".
Use the option "FileETag MTime Size" if you just want to remove the Inode information.

OpenBSD:

OpenBSD has released a patch that fixes this vulnerability. After installing the patch, inode numbers returned from the server are encoded using a private hash to avoid the release of sensitive information.

Results:

```
22145-7dc-51a27a9100780
```

Type: **Web Application**

INFO

Server accepts unnecessarily large POST request body

QID: 150086 **CVSS Base:**
Category: Web Application **Port: -**
CVEID: -

Threat:

Web application scanner successfully sent a POST request with content type of application/x-www-form-urlencoded and 65536 bytes length random text data. Accepting request bodies with unnecessarily large size could help attacker to use less connections to achieve Layer 7 DDoS of web server. More information can be found at the here

Impact:

Could result in successful application level (Layer 7) DDoS attack.

Solution:

Limit the size of the request body to each form's requirements. For example, a search form with 256-char search field should not accept more than 1KB value. Server-specific details can be found here .

Results:

```
https://fdago.conceptplusllc.net -- Server responded 200 to
unnecessarily large random request body(over 64 KB) for URL
https://fdago.conceptplusllc.net/, significantly increasing
attacker's chances to prolong slow HTTP POST attack.
```

Type: **Vulnerability**

INFO

DEFLATE Data Compression Algorithm Used for HTTPS

QID: 42416 **CVSS Base:**
Category: General remote services **Port: 0**
CVEID: -

Threat:
HTTP data is compressed before it is sent from the server. DEFLATE data compression algorithm uses the LZ77 algorithm which takes advantage of repeated strings to more efficiently compress output.
DEFLATE data compression algorithm is prone to be unsafe as described in the BREACH attack. If an attacker can inject a string into a HTTPS response intended to match another unknown string (the target secret), they can iteratively guess the secret value by monitoring the compressed size of the responses for different guesses. Note: The attacker needs the capability of reading responses received by the user's browser and the capability of cause the victim to send requests from their browser to perform BREACH attack.
This QID detects that the remote HTTP server is using a gzip or DEFLATE (zlib) compression format which is using DEFLATE data compression algorithm.

Impact:
N/A

Solution:
N/A

Results:

```
HTTP/1.1 200 OK Accept-Ranges: bytes Content-Encoding: gzip Content-
Type: text/html Date: Mon, 06 Jul 2015 16:47:07 GMT ETag: "22145-
7dc-51a27a9100780" Last-Modified: Sun, 05 Jul 2015 21:42:06 GMT
Server: Apache/2.2.22 (Ubuntu) Vary: Accept-Encoding Content-Length:
978 Connection: keep-alive
_1F_8B_08_00_00_00_00_00_00_03_A5UKo_DBF_10_BE_E7W_8C_D9_83$_94_8F
qk;%_05(u_DA_E6_92_16E_0B_A40t_18-
_87_E4_BA_AB]vw)E_88_F3_DF;_CB_87,_AB_06Z_A0:h_B8_F3_E2_CC_B73_1F_F3
_8B_D2_08_7Fh
_1A_BFUK_C8_83_00_A1_D0_B9"_D2&_B9wQP_12_96,_B6_E4_11D_83_D6_91/_A2_
CEW_C9u_B0z_E9_15-_F3l_90_A3_9B_C6-
_15QINX_D9zit_04_C2hO_9A#_A3_A7N;I_FB_D6X_7F_E2_B1_97_A5o_8A_92vRP_D
2_1FB_CCE_92_C0/ _05A_85l1:_E5?
@]_02_B6_AD_A2_C4_9BN4IohuR_83o_08_AC1_1EJiIxc_0F_90$_9CII_FD'XRE_E4
_FCA_91k_88_F8_F5_8D_A5j_D2d;_D2_A5_B1iyus_8DXQ*\_0F_C5_7F_88_DC_A2_
D4)_BD_C6_CB_EB_CB_CBj_8C_83|c_CA_03_E8:_E1R_8B_A8*_B16_AB_B6_1D_BB_
BA_93_15(_0F_EF_DF_C1_D5z_F9_02_FA__DEN_D7_B0_B1f_EF_A8_E1_C0C_B4_FC
_C3t_80_96_A0s_92[D_B9_F3_D6_E8zi:__A2_A72_CFF_05_0Cq6e_CC_08_1DA_8E
c_9D_8D_F7_ED_9B,;_C9_9B
_B3_CD_A2e_D7_D6_16K_82_83_E9_EC_14_9Eg_B8_04o@n[kv_A3_8D>_B5d%iAi_9
E_B5C_C9_F9_C5_1DC&_ABu_8Fp_B8_AB_iG_A8`K_BA_1B`/_E5_EE8[_B8_EB_F5_A
3LJ_AA_B0c_0C_A6s%?
Q_99(_AA|_C0_08_CF_C2_92_8D_E5k_9Fp_FF_8AK_FF_C9l_A9/5_EF_D4_89_F31_
1F_CB_E1_FA_96G_18R_0E_BB_B5]_CDu T_CA_85_F0<c_8Fg_DC_FAI|_D6qz_19
/w_14=_8D_FB_C1_98_F2_99_A8_AC_0B_AB_961_1COA_11_A8w_D8_8FYP_CA_B2oA
_D68_EE_CF_B1_ABZ_18_C4)n_E18_C0_E6M?
Y_9B_CE{_C3K_C0_EB_CDS_D4_1F_CE_B2_B0g]+_8A_80G_07_C7C_11_99_AA_1A+_
19_F464 xjQ_B9_A3/_DA:_B0@:_02<_AA_878V?
```

_B6_E2Z_9E_D2_F1_ADa7_13~/_C3_94_05_FD_FF6gC[_CF_A3_C9l_C2_ABHv_02_9
4_B7/pM _A0_C9_FD_9FQ_15_D3_C5c_C8y*_10_CCO_83_B9]>)_AEV_87_B6
_15_C2_F1)a_DEdZ;V[Y_B3_ED)_E9{_C3_9B_D3z^_CC_CE_81'_DC_86%_82_B3_9A
F_11_16_E9Gc_F8b`_A5Q_1D_BC_14_EEM`a]_13_FC_BEJ>_86__F21_AC_E8f_DCN'
=_CD_1C_BC_BF_1D_B6n_A0_E0_E5E_D5i_11&i_BE_8Au_C7]_ACb_8C_ED_E2_F3*
_1D_F2_1F_D3_FF_BC_B9g_B2,T_BC_BAS_EB"_FC=
<_1C_83_17_9FG_82_82y_B0_A4_7F_15_83xx_B8[/_D2_B6s_CD_9CG_A3_E3_99_F
0n_F1_A5O_91_AA_E2kM{_B8e~_8A_B1_D0_A9_B0_C4_8F_EF_14_05_AFy_BD_88_A
7_94_96_8D<V_A3_C5_BD=_FC_86_F5_07_FEH_B0_CF_DD_CBu_8C_A9_B3_A2_E8b_
9B_B6_CC_81_DA_7F0%_A5R3K_F9_B7T_19K_F3_D0_D0_94_EC_CB|/_99_C3_F71_7
F_E2_FAz_E2_D9_00_C5,_9Ee_D9~_BFO_EB_BE_EF_04_A7_C6{_1A|
<_DD;_F6_ACq_B6_F8_EE_C5_94_B3_C6_F9l_A8~_16_C3_EC_11_FE_E0s_E2_E2_9
8
_83C_8B5_85_91c3_0F_C1p_0F_D3_85@_E8%_1A_9E_8F_9F_1B|uu_F3_AD_F8_E6U
_1A>_BC_FF_122_CA_147/77_AF_AFn_CEb_E0o[_98_8C_F0_DC_07 HTTP/1.1 200
OK Accept-Ranges: bytes Content-Encoding: gzip Content-Type:
text/html Date: Mon, 06 Jul 2015 16:47:32 GMT ETag: "22145-7dc-
51a27a9100780" Last-Modified: Sun, 05 Jul 2015 21:42:06 GMT Server:
Apache/2.2.22 (Ubuntu) Vary: Accept-Encoding Content-Length: 978
Connection: keep-alive
_1F_8B_08_00_00_00_00_00_00_03_A5UKo_DBF_10_BE_E7W_8C_D9_83$_94_8F
qk;%_05(u_DA_E6_92_16E_0B_A40t_18-
_87_E4_BA_AB]vw)E_88_F3_DF;_CB_87,_AB_06Z_A0:h_B8_F3_E2_CC_B73_1F_F3
_8B_D2_08_7Fh
_1A_BFUK_C8_83_00_A1_D0_B9"_D2&_B9wQP_12_96,_B6_E4_11D_83_D6_91/_A2_
CEW_C9u_B0z_E9_15-_F3l_90_A3_9B_C6-
_15QINX_D9zit_04_C2hO_9A#_A3_A7N;I_FB_D6X_7F_E2_B1_97_A5o_8A_92vRP_D
2_1FB_CCE_92_C0/ _05A_85l1:_E5?
@]_02_B6_AD_A2_C4_9BN4IohuR_83o_08_AC1_1EJiIxc_0F_90$_9CII_FD'XRE_E4
_FCA_91k_88_F8_F5_8D_A5j_D2d;_D2_A5_B1iyus_8DXQ*_0F_C5_7F_88_DC_A2_
D4)_BD_C6_CB_EB_CB_CBj_8C_83|c_CA_03_E8:_E1R_8B_A8*_B16_AB_B6_1D_BB_
BA_93_15(_0F_EF_DF_C1_D5z_F9_02_FA__DEN_D7_B0_B1f_EF_A8_E1_C0C_B4_FC
_C3t_80_96_A0s_92[D_B9_F3_D6_E8zi:__A2_A72_CFF_05_0Cq6e_CC_08_1DA_8E
c_9D_8D_F7_ED_9B,;_C9_9B
_B3_CD_A2e_D7_D6_16K_82_83_E9_EC_14_9Eg_B8_04o@n[kv_A3_8D>_B5d%iAi_9
E_B5C_C9_F9_C5_1DC&_ABu_8Fp_B8_AB_iG_A8`K_BA_1B`/_E5_EE8[_B8_EB_F5_A
3LJ_AA_B0c_0C_A6s%?
Q_99(_AA|_C0_08_CF_C2_92_8D_E5k_9Fp_FF_8AK_FF_C9l_A9/5_EF_D4_89_F31_
1F_CB_E1_FA_96G_18R_0E_BB_B5]_CDu T_CA_85_F0<c_8Fg_DC_FAI|_D6qz_19
/w_14=_8D_FB_C1_98_F2_99_A8_AC_0B_AB_961_1COA_11_A8w_D8_8FYP_CA_B2oA
_D68_EE_CF_B1_ABZ_18_C4)n_E18_C0_E6M?
Y_9B_CE{_C3K_C0_EB_CDS_D4_1F_CE_B2_B0g]+_8A_80G_07_C7C_11_99_AA_1A+_
19_F464 xjQ_B9_A3/_DA:_B0@:_02<_AA_878V?
_B6_E2Z_9E_D2_F1_ADa7_13~/_C3_94_05_FD_FF6gC[_CF_A3_C9l_C2_ABHv_02_9
4_B7/pM _A0_C9_FD_9FQ_15_D3_C5c_C8y*_10_CCO_83_B9]>)_AEV_87_B6
_15_C2_F1)a_DEdZ;V[Y_B3_ED)_E9{_C3_9B_D3z^_CC_CE_81'_DC_86%_82_B3_9A
F_11_16_E9Gc_F8b`_A5Q_1D_BC_14_EEM`a]_13_FC_BEJ>_86__F21_AC_E8f_DCN'
=_CD_1C_BC_BF_1D_B6n_A0_E0_E5E_D5i_11&i_BE_8Au_C7]_ACb_8C_ED_E2_F3*
_1D_F2_1F_D3_FF_BC_B9g_B2,T_BC_BAS_EB"_FC=
<_1C_83_17_9FG_82_82y_B0_A4_7F_15_83xx_B8[/_D2_B6s_CD_9CG_A3_E3_99_F
0n_F1_A5O_91_AA_E2kM{_B8e~_8A_B1_D0_A9_B0_C4_8F_EF_14_05_AFy_BD_88_A
7_94_96_8D<V_A3_C5_BD=_FC_86_F5_07_FEH_B0_CF_DD_CBu_8C_A9_B3_A2_E8b_
9B_B6_CC_81_DA_7F0%_A5R3K_F9_B7T_19K_F3_D0_D0_94_EC_CB|/_99_C3_F71_7
F_E2_FAz_E2_D9_00_C5,_9Ee_D9~_BFO_EB_BE_EF_04_A7_C6{_1A|
<_DD;_F6_ACq_B6_F8_EE_C5_94_B3_C6_F9l_A8~_16_C3_EC_11_FE_E0s_E2_E2_9
8
_83C_8B5_85_91c3_0F_C1p_0F_D3_85@_E8%_1A_9E_8F_9F_1B|uu_F3_AD_F8_E6U
_1A>_BC_FF_122_CA_147/77_AF_AFn_CEb_E0o[_98_8C_F0_DC_07

INFO

Web Server Probed For Various URL-Encoding Schemes Supported

QID: 12059 **CVSS Base:**

Category: CGI **Port: 443**
CVEID: -

Threat:
The target Web server was probed for various URL-encoding schemes that it supports.
Per this paper by Daniel Roelker that was presented at Defcon 11, popular Web servers like Microsoft IIS support a variety of encoding schemes for the URLs. These include Percent-escaped Hex Encoding, Double-percent Escaped Hex Encoding, Microsoft's %U Encoding, Percent-escaped 2-Byte UTF-8 Encoding, and Raw 2-Byte UTF-8 Encoding.
For a sample HTTP GET request, GET /. HTTP/1.0, the following illustrates the encoded URI under these schemes:
`Percent-escaped Hex Encoding: GET /%2e HTTP/1.0 Double-percent Escaped Hex Encoding: GET /%252e HTTP/1.0 Percent-escaped 2-Byte UTF-8 Encoding: GET /%C0%AE HTTP/1.0 Raw 2-Byte UTF-8 Encoding: GET /\xC0\xAE HTTP/1.0 (Actual raw 0xC0 and 0xAE bytes) Microsoft's %U Encoding: GET /%u002e HTTP/1.0`
The supported encoding schemes are listed in the Results section.
URI encoding is relevant to Web server security since, as mentioned in the paper above, attackers could launch HTTP attacks while at the same time obfuscating the URIs to evade detection by Intrusion Detection Systems that are not capable of decoding the URIs.

Impact:
N/A

Solution:
N/A

Results:
`Single-%-Escaped Hex-Encoding Supported`

INFO

Web Server Probed For Various URL-Encoding Schemes Supported

QID: 12059 **CVSS Base:**
Category: CGI **Port: 80**
CVEID: -

Threat:
The target Web server was probed for various URL-encoding schemes that it supports.
Per this paper by Daniel Roelker that was presented at Defcon 11, popular Web servers like Microsoft IIS support a variety of encoding schemes for the URLs. These include Percent-escaped Hex Encoding, Double-percent Escaped Hex Encoding, Microsoft's %U Encoding, Percent-escaped 2-Byte UTF-8 Encoding, and Raw 2-Byte UTF-8 Encoding.
For a sample HTTP GET request, GET /. HTTP/1.0, the following illustrates the encoded URI under these schemes:
`Percent-escaped Hex Encoding: GET /%2e HTTP/1.0 Double-percent Escaped Hex Encoding: GET /%252e HTTP/1.0 Percent-escaped 2-Byte UTF-8 Encoding: GET /%C0%AE HTTP/1.0 Raw 2-Byte UTF-8 Encoding: GET /\xC0\xAE HTTP/1.0 (Actual raw 0xC0 and 0xAE bytes) Microsoft's %U Encoding: GET /%u002e HTTP/1.0`
The supported encoding schemes are listed in the Results section.
URI encoding is relevant to Web server security since, as mentioned in the paper above, attackers could launch HTTP attacks while at the same time obfuscating the URIs to evade detection by Intrusion Detection Systems that are not capable of decoding the URIs.

Impact:
N/A

Solution:
N/A

Results:
`Single-%-Escaped Hex-Encoding Supported`

INFO

Firewall Detected

QID: 34011 **CVSS Base:**
Category: Firewall **Port: 0**
CVEID: -

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).

Impact:

Solution:

Results:
```
Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25,
53, 111, 135, 445, 1. Listed below are the ports filtered by the
firewall. No response has been received when any of these ports is
probed. 1-3,5,7,9,11,13,15,17-25,27,29,31,33,35,37-39,41-79,81-
223,242-246,256-265, 280-282,309,311,318,322-325,344-351,363,369-
381,383-442,444-581,587,592-593, 598,600,606-620,624,627,631,633-
637,666-674,700,704-705,707,709-711,729-731, 740-742,744,747-
754,758-765,767,769-777,780-783,786,799-801,860,873,886-888, 900-
901,911,950,954-955,990-993,995-1001,1008,1010-1011,1015,1023-1100,
1109-1112,1114,1123,1155,1167,1170,1207,1212,1214,1220-1222,1234-
1236, 1241,1243,1245,1248,1269,1313-1314,1337,1344-1625,1636-
1774,1776-1815, 1818-1824,1900-1909,1911-1920,1944-
1951,1973,1981,1985-2028,2030,2032-2036, 2038,2040-
2049,2053,2065,2067,2080,2097,2100,2102-2107,2109, and more. We have
omitted from this list 698 higher ports to keep the report size
manageable.
```

INFO

Open TCP Services List

QID: 82023 **CVSS Base:**
Category: TCP/IP **Port: 0**
CVEID: -

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.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

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 .

Results:
```
#table cols="5" 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 _
```

INFO

SSL Web Server Version

QID: 86001
Category: Web server
CVEID: -
CVSS Base:
Port: 443

Threat:

Impact:

Solution:

Results:
```
#table cols="2" Server_Version Server_Banner Apache/2.2.22_(Ubuntu)
Apache/2.2.22_(Ubuntu)
```

INFO

Web Server Version

QID: 86000
Category: Web server
CVEID: -
CVSS Base:
Port: 80

Threat:
N/A

Impact:
N/A

Solution:
N/A

Results:
```
#table cols="2" Server_Version Server_Banner Apache/2.2.22_(Ubuntu)
Apache/2.2.22_(Ubuntu)
```

INFO

Internet Service Provider

QID: 45005
Category: Information gathering
CVEID: -
CVSS Base:
Port: 0

Threat:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

Impact:
This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

Solution:
N/A

Results:
```
The ISP network handle is: AMAZON-05 ISP Network description:
Amazon.com, Inc.
```

INFO

Default Web Page

QID: 12230 **CVSS Base:**
Category: CGI **Port: 443**
CVEID: -

Threat:
The Result section displays the default Web page for the Web server.

Impact:
N/A

Solution:
N/A

Results:
```
HTTP/1.1 200 OK Accept-Ranges: bytes Content-Type: text/html Date:
Mon, 06 Jul 2015 16:45:16 GMT ETag: "22145-7dc-51a27a9100780" Last-
Modified: Sun, 05 Jul 2015 21:42:06 GMT Server: Apache/2.2.22
(Ubuntu) Vary: Accept-Encoding Content-Length: 2012 Connection:
keep-alive <!doctype html> <html class="no-js"> <head> <meta
charset="utf-8"> <title></title> <meta name="description"
content=""> <meta name="viewport" content="width=device-width"> <!--
Place favicon.ico and apple-touch-icon.png in the root directory -->
<link rel="stylesheet" href="styles/vendor.d798aafe.css"> <link
rel="stylesheet" href="styles/main.e3a4844f.css"> <body ng-
app="fdagoApp"> <!--[if lt IE 7]> <p class="browsehappy">You are
using an <strong>outdated</strong> browser. Please <a
href="http://browsehappy.com/">upgrade your browser</a> to improve
your experience.</p> <![endif]--> <!-- Reveal menu --> <div
class="navmenu navmenu-default navmenu-fixed-left"> <a
class="navmenu-brand" href="#/">Home</a> <ul class="nav navmenu-
nav"> <li><a href="./">Drug Recalls</a></li> <li><a href="./">Device
Recalls</a></li> <li class="active"><a href="./">Food Recalls</a>
</li> </ul> </div> <div class="canvas"> <div id="navigation"
class="navbar navbar-default navbar-fixed-top"> <button
type="button" class="navbar-toggle" data-toggle="offcanvas" data-
recalc="false" data-target=".navmenu" data-canvas=".canvas"> <span
class="icon-bar"></span> <span class="icon-bar"></span> <span
class="icon-bar"></span> </button> </div> <div class="container">
<div ng-view=""></div> </div> <div class="footer"> <div
class="container center"> <p><span class="glyphicon glyphicon-
heart"></span> from the Concept Plus team</p> </div> </div> </div>
<!-- Google Analytics: change UA-XXXXX-X to be your site's ID -->
<script>!function(A,n,g,u,l,a,r)
{A.GoogleAnalyticsObject=l,A[l]=A[l]||function(){ (A[l].q=A[l].q||
[]).push(arguments)},A[l].l=+new Date,a=n.createElement(g),
r=n.getElementsByTagName(g)
[0],a.src=u,r.parentNode.insertBefore(a,r) }
(window,document,'script','//www.google-
analytics.com/analytics.js','ga'); ga('create', 'UA-XXXXX-X');
ga('send', 'pageview');</script> <script
src="scripts/vendor.a2796c52.js"></script> <script
src="scripts/scripts.ab0b9379.js"></script>
```

INFO

TLS Secure Renegotiation Extension Supported

QID: 42350 **CVSS Base:**
Category: General remote services **Port: 443**
CVEID: -

Threat:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over, This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

Impact:
N/A

Solution:
N/A

Results:
```
TLS Secure Renegotiation Extension Status: supported.
```

INFO

SSL Session Caching Information

QID: 38291 **CVSS Base:**
Category: General remote services **Port: 443**
CVEID: -

Threat:
SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

Impact:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

Solution:

Results:
```
TLSv1 session caching is enabled on the target.
```

INFO

SSL Certificate - Information

QID: 86002 **CVSS Base:**
Category: Web server **Port: 443**
CVEID: -

Threat:

Impact:

Solution:

Results:
```
#table cols="2" NAME VALUE (0)CERTIFICATE_0 _ (0)Version 3_(0x2)
(0)Serial_Number _fa:e0:de:9d:4b:4f:0c:ee_ (0)Signature_Algorithm
sha256WithRSAEncryption (0)ISSUER_NAME _ countryName US
_stateOrProvinceName Arizona _localityName Scottsdale
```

```
_organizationName "GoDaddy.com,_Inc." _organizationalUnitName
http://certs.godaddy.com/repository/ _commonName
Go_Daddy_Secure_Certificate_Authority_-_G2 (0)SUBJECT_NAME _
organizationalUnitName Domain_Control_Validated _commonName
*.conceptplusllc.net (0)Valid_From May_6_01:49:38_2015_GMT
(0)Valid_Till May_6_01:49:38_2016_GMT (0)Public_Key_Algorithm
rsaEncryption (0)RSA_Public_Key (2048_bit) (0) _Public-
Key:_(2048_bit) (0) _Modulus: (0)
_00:e8:db:1c:2f:fb:df:0d:84:b4:5d:f8:fe:3a:85: (0)
_75:91:76:4e:ea:09:a3:5c:e8:c3:0a:f4:59:9a:14: (0)
_3b:e0:32:cc:2a:ec:04:9e:1c:a4:84:51:4e:df:69: (0)
_fe:62:0b:7e:87:91:e0:75:b5:18:2f:83:02:c0:63: (0)
_65:b7:a6:17:be:6b:c0:c6:dd:bf:90:b9:b1:7e:fc: (0)
_dd:70:d3:e1:ce:2f:ee:8d:59:07:f6:59:39:0e:e6: (0)
_25:69:40:ef:87:84:25:ea:16:b1:ea:44:03:66:0b: (0)
_b8:56:dd:d0:ba:2a:14:e8:a9:8e:a6:26:69:3d:5e: (0)
_ef:e0:cf:c0:ad:1a:47:0b:32:6d:b2:c7:c6:83:0c: (0)
_a7:e7:8b:ba:d8:76:7b:49:55:dd:47:0e:c5:75:0f: (0)
_ec:00:2f:6b:f8:2a:8e:cf:31:ad:58:7b:1a:ca:96: (0)
_01:f6:34:b4:0f:6b:22:40:ee:6c:8e:65:6e:72:2d: (0)
_11:0e:af:66:8b:8f:17:d1:fc:27:a1:c5:4f:d6:5a: (0)
_5a:93:82:98:9e:4e:d5:73:f5:31:44:06:f2:a6:9f: (0)
_e7:15:f7:c1:41:cf:f8:fb:e1:66:39:74:03:9e:c5: (0)
_57:c3:c3:4c:b8:89:1e:17:14:14:a7:41:2e:10:9e: (0)
_01:83:70:ba:e9:35:f2:5c:06:d8:5a:74:75:06:e0: (0) _15:a1 (0)
_Exponent:_65537_(0x10001) (0)X509v3_EXTENSIONS _
(0)X509v3_Basic_Constraints critical (0) _CA:FALSE
(0)X509v3_Extended_Key_Usage
_TLS_Web_Server_Authentication,_TLS_Web_Client_Authentication
(0)X509v3_Key_Usage critical (0)
_Digital_Signature,_Key_Encipherment
(0)X509v3_CRL_Distribution_Points (0) _Full_Name: (0)
_URI:http://crl.godaddy.com/gdig2s1-87.crl
(0)X509v3_Certificate_Policies _Policy:_2.16.840.1.114413.1.7.23.1
(0) _CPS:_http://certificates.godaddy.com/repository/
(0)Authority_Information_Access _OCSP_-_URI:http://ocsp.godaddy.com/
(0) _CA_Issuers_-
_URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3_Authority_Key_Identifier
_keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3_Subject_Alternative_Name
_DNS:*.conceptplusllc.net,_DNS:conceptplusllc.net
(0)X509v3_Subject_Key_Identifier
_ED:87:95:12:94:D0:E4:5B:9F:98:1F:03:9A:40:C6:97:D2:AB:2A:7D
(0)Signature (256_octets) (0)
b7:27:bf:79:f3:0e:ff:7c:cf:66:97:a5:40:06:13:0b (0)
f7:d6:46:30:2f:c9:01:d9:e0:9b:c3:ac:42:b8:90:5d (0)
b6:ef:f2:c0:8d:57:e7:c5:49:9b:46:f8:8e:ea:43:84 (0)
80:b0:da:7a:71:61:9f:3e:64:6f:bf:1d:f0:c4:bd:b1 (0)
0b:44:8c:45:d9:56:16:64:74:8a:e4:f5:a5:2e:6b:ee (0)
71:99:5d:56:f4:ef:e4:01:8c:41:e9:c6:dd:0a:81:60 (0)
31:57:7e:5b:e6:30:d5:f2:a1:54:a9:d1:b0:7c:e2:92 (0)
be:2b:a9:c7:d0:dd:05:f5:49:44:e3:6a:29:5e:43:1a (0)
62:9a:00:00:9f:2c:96:0c:24:65:da:ff:74:cc:33:f7 (0)
f8:95:10:b3:7a:65:d2:8f:01:55:48:51:3a:08:bd:a9 (0)
44:4c:d7:42:12:0a:5e:b7:58:92:11:f2:05:5d:62:83 (0)
c1:59:df:1d:6f:e6:7d:7f:d0:01:63:75:c4:f5:a3:7c (0)
e4:7b:7e:33:a4:7e:49:de:31:4a:4e:2f:b8:bc:d6:e9 (0)
f9:bb:1a:56:4c:4b:cb:83:17:7d:b3:26:54:76:73:9f (0)
56:83:d3:3f:7c:72:f4:07:88:65:fd:89:5e:2a:27:44 (0)
e8:4a:7f:fa:ce:43:8f:d2:84:1c:92:0c:0a:b5:10:73
```

INFO

Host Names Found

QID: 45039 **CVSS Base:**
Category: Information gathering **Port: 0**
CVEID: -

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.

Impact:
N/A

Solution:
N/A

Results:
```
#table cols="2" Host_Name Source fdago.conceptplusllc.net User-provided_DNS ec2-54-164-73-28.compute-1.amazonaws.com FQDN
```

INFO

SSL/TLS invalid protocol version tolerance

QID: 38597 **CVSS Base:**
Category: General remote services **Port: 443**
CVEID: -

Threat:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the targets behavior. The results section contains a table that indicates what was the target's response to each of our tests.

Impact:
N/A

Solution:
N/A

Results:
```
#table cols=2 my_version target_version 0304 0303 0399 0303 0400 rejected 0499 rejected
```

INFO

SSL/TLS Server supports TLS_FALLBACK_SCSV

QID: 38610 **CVSS Base:**
Category: General remote services **Port: 443**
CVEID: -

Threat:
TLS cipher suite TLS_FALLBACK_SCSV is a signaling cipher suite value (SCSV). TLS servers support TLS_FALLBACK_SCSV will prevent downgrade attack.

Impact:
N/A

Solution:
N/A

Results:
```
TLS_FALLBACK_SCSV is supported on port 443.
```

INFO

Degree of Randomness of TCP Initial Sequence Numbers

QID: 82045 **CVSS Base:**
Category: TCP/IP **Port: 0**
CVEID: -

Threat:
TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

Impact:
N/A

Solution:
N/A

Results:
```
Average change between subsequent TCP initial sequence numbers is
1463865829 with a standard deviation of 769897400. These TCP initial
sequence numbers were triggered by TCP SYN probes sent to the host
at an average rate of 1/(6790 microseconds). The degree of
difficulty to exploit the TCP initial sequence number generation
scheme is: hard.
```

INFO

List of Web Directories

QID: 86672 **CVSS Base:**
Category: Web server **Port: 80**
CVEID: -

Threat:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

Impact:

Solution:

Results:
```
#table cols="2" Directory Source /cgi-bin/ brute_force /scripts/
brute_force /doc/ brute_force /images/ brute_force /scripts/
web_page /icons/ web_page /styles/ web_page /images/ web_page
```

INFO

DNS Host Name

QID: 6 **CVSS Base: 0**
Category: Information gathering **Port: 0**
CVEID: -

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

Impact:

Solution:

Results:
```
#table IP_address Host_name 54.164.73.28 fdago.conceptplusllc.net
54.164.73.28 ec2-54-164-73-28.compute-1.amazonaws.com
```

INFO

SSL Server Information Retrieval

QID: 38116 **CVSS Base:**
Category: General remote services **Port: 443**
CVEID: -

Threat:
The following is a list of supported SSL ciphers. **Note:** If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

Impact:
N/A

Solution:
N/A

Results:
```
#table cols="6" CIPHER KEY-EXCHANGE AUTHENTICATION MAC
ENCRYPTION(KEY-STRENGTH) GRADE SSLv2_PROTOCOL_IS_DISABLED _ _ _ _ _
SSLv3_PROTOCOL_IS_DISABLED _ _ _ _ _ TLSv1_PROTOCOL_IS_ENABLED _ _ _
_ _ TLSv1 COMPRESSION_METHOD None _ _ _ DES-CBC3-SHA RSA RSA SHA1
3DES(168) _HIGH_ AES128-SHA RSA RSA SHA1 AES(128) _MEDIUM_ AES256-
SHA RSA RSA SHA1 AES(256) _HIGH_ ECDHE-RSA-AES128-SHA ECDH RSA SHA1
AES(128) _MEDIUM_ ECDHE-RSA-AES256-SHA ECDH RSA SHA1 AES(256) _HIGH_
```

INFO

Host Scan Time

QID: 45038 **CVSS Base:**
Category: Information gathering **Port: 0**
CVEID: -

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.

Impact:
N/A

Solution:
N/A

Results:
```
Scan duration: 641 seconds Start time: Mon, Jul 06 2015, 16:37:43
GMT End time: Mon, Jul 06 2015, 16:48:24 GMT
```

INFO

IP ID Values Randomness

QID: 82046
Category: TCP/IP
CVEID: -
CVSS Base:
Port: 0

Threat:
The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.
Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

Impact:
N/A

Solution:
N/A

Results:
```
IP ID changes observed (network order) for port 80: 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 Duration: 66 milli seconds
```

INFO

Default Web Page

QID: 12230
Category: CGI
CVEID: -
CVSS Base:
Port: 80

Threat:
The Result section displays the default Web page for the Web server.

Impact:
N/A

Solution:
N/A

Results:
```
HTTP/1.1 200 OK Accept-Ranges: bytes Content-Type: text/html Date:
Mon, 06 Jul 2015 16:43:01 GMT ETag: "22145-7dc-51a27a9100780" Last-
Modified: Sun, 05 Jul 2015 21:42:06 GMT Server: Apache/2.2.22
(Ubuntu) Vary: Accept-Encoding Content-Length: 2012 Connection:
keep-alive <!doctype html> <html class="no-js"> <head> <meta
charset="utf-8"> <title></title> <meta name="description"
content=""> <meta name="viewport" content="width=device-width"> <!--
Place favicon.ico and apple-touch-icon.png in the root directory -->
<link rel="stylesheet" href="styles/vendor.d798aafe.css"> <link
rel="stylesheet" href="styles/main.e3a4844f.css"> <body ng-
app="fdagoApp"> <!--[if lt IE 7]> <p class="browsehappy">You are
using an <strong>outdated</strong> browser. Please <a
href="http://browsehappy.com/">upgrade your browser</a> to improve
your experience.</p> <![endif]--> <!-- Reveal menu --> <div
class="navmenu navmenu-default navmenu-fixed-left"> <a
class="navmenu-brand" href="#/">Home</a> <ul class="nav navmenu-
nav"> <li><a href="./">Drug Recalls</a></li> <li><a href="./">Device
```

```
Recalls</a></li> <li class="active"><a href="./">Food Recalls</a>
</li> </ul> </div> <div class="canvas"> <div id="navigation"
class="navbar navbar-default navbar-fixed-top"> <button
type="button" class="navbar-toggle" data-toggle="offcanvas" data-
recalc="false" data-target=".navmenu" data-canvas=".canvas"> <span
class="icon-bar"></span> <span class="icon-bar"></span> <span
class="icon-bar"></span> </button> </div> <div class="container">
<div ng-view=""></div> </div> <div class="footer"> <div
class="container center"> <p><span class="glyphicon glyphicon-
heart"></span> from the Concept Plus team</p> </div> </div> </div>
<!-- Google Analytics: change UA-XXXXX-X to be your site's ID -->
<script>!function(A,n,g,u,l,a,r)
{A.GoogleAnalyticsObject=l,A[l]=A[l]||function(){ (A[l].q=A[l].q||
[]).push(arguments)},A[l].l=+new Date,a=n.createElement(g),
r=n.getElementsByTagName(g)
[0],a.src=u,r.parentNode.insertBefore(a,r) }
(window,document,'script','//www.google-
analytics.com/analytics.js','ga'); ga('create', 'UA-XXXXX-X');
ga('send', 'pageview');</script> <script
src="scripts/vendor.a2796c52.js"></script> <script
src="scripts/scripts.ab0b9379.js"></script>
```

INFO

HTTP Methods Returned by OPTIONS Request

QID: 45056 **CVSS Base:**
Category: Information gathering **Port: 443**
CVEID: -

Threat:
The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

Impact:
N/A

Solution:
N/A

Results:
```
Allow: GET,HEAD,POST,OPTIONS
```

INFO

List of Web Directories

QID: 86672 **CVSS Base:**
Category: Web server **Port: 443**
CVEID: -

Threat:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

Impact:

Solution:

Results:
```
#table cols="2" Directory Source /cgi-bin/ brute_force /scripts/
brute_force /doc/ brute_force /images/ brute_force /scripts/
web_page /icons/ web_page /styles/ web_page /images/ web_page
```

INFO

Target Network Information

QID: 45004 **CVSS Base:**
Category: Information gathering **Port: 0**
CVEID: -

Threat:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

Impact:
This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.

Solution:
N/A

Results:
```
The network handle is: AMAZON-2011L Network description: Amazon
Technologies Inc.
```

INFO

Traceroute

QID: 45006 **CVSS Base:**
Category: Information gathering **Port: 0**
CVEID: -

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.

Impact:

Solution:

Results:
```
#table cols="4" Hops IP Round_Trip_Time Probe 1 64.39.103.251 0.37ms
ICMP 2 216.35.14.45 0.01ms ICMP 3 216.33.4.77 0.56ms ICMP 4
204.70.207.30 0.01ms ICMP 5 204.70.207.37 2.03ms ICMP 6
204.70.192.89 22.83ms ICMP 7 206.28.97.246 13.44ms ICMP 8
63.235.40.85 13.55ms ICMP 9 67.14.28.110 82.81ms ICMP 10
72.165.86.74 87.88ms ICMP 11 54.239.109.190 85.54ms ICMP 12
54.239.109.183 89.40ms ICMP 13 205.251.245.246 84.09ms ICMP 14
*.*.*.* 0.00ms Other 15 *.*.*.* 0.00ms Other 16 *.*.*.* 0.00ms Other
17 54.164.73.28 82.93ms TCP
```

INFO

HTTP Methods Returned by OPTIONS Request

QID: 45056 **CVSS Base:**
Category: Information gathering **Port: 80**
CVEID: -

Threat:
The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

Impact:
N/A

Solution:
N/A

Results:
```
Allow: GET,HEAD,POST,OPTIONS
```