QUALYS ENTERPRISE

Scan Results

April 27, 2017

This report was generated with an evaluation version of Qualys

Report Summary

User Name:	Mark Sanders
Login Name:	de2ms
Company:	Dell
User Role:	Manager
Address:	652 Peachtree Valley Drive
City:	Roanoke
State:	Virginia
Zip:	24012
Country:	United States of America
Created:	04/27/2017 at 11:17:37 (GMT+0530)
Launch Date:	04/27/2017 at 10:50:38 (GMT+0530)
Active Hosts:	1
Total Hosts:	1
Type:	On demand
Status:	Finished
Reference:	scan/1493270267.04998
Scanner Appliances:	ChennaiScanner (Scanner 9.2.33-1, Vulnerability Signatures 2.4.27-2)
Duration:	00:25:36
Title:	AFM_CPS_74_2
Asset Groups:	-
IPs:	10.16.133.74
Excluded IPs:	-
Options Profile:	d-scan-full-1

Summary of Vulnerabilities

Vulnerabilities Total	49

Security Risk (Avg)	2.0

by Severity

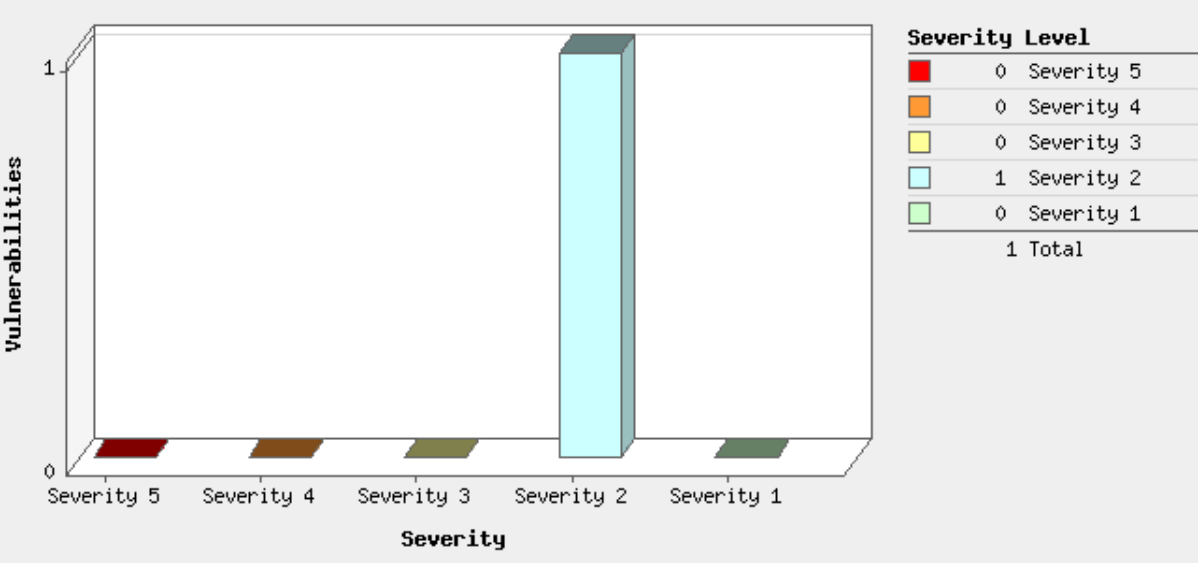
Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	0	0	0	0
3	0	0	1	1
2	1	0	8	9
1	0	0	39	39
Total	1	0	48	49

5 Biggest Categories

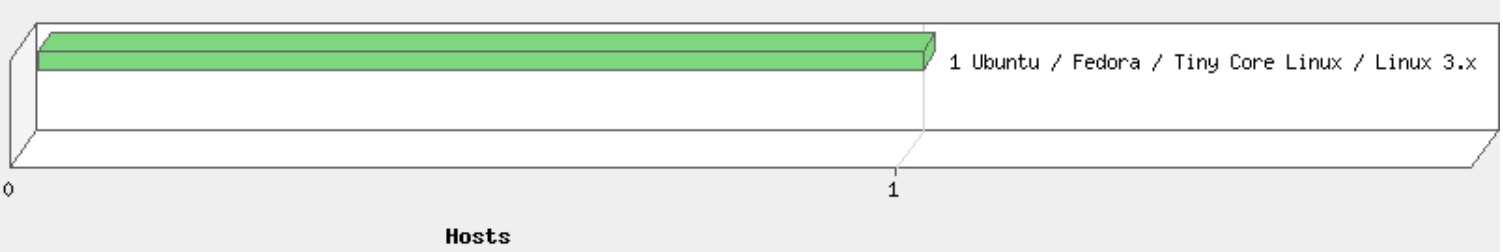
Category	Confirmed	Potential	Information Gathered	Total
Information gathering	0	0	13	13
Web server	0	0	12	12
General remote services	1	0	8	9
CGI	0	0	7	7
TCP/IP	0	0	6	6

Category	Confirmed	Potential	Information Gathered	Total
Total	1	0	46	47

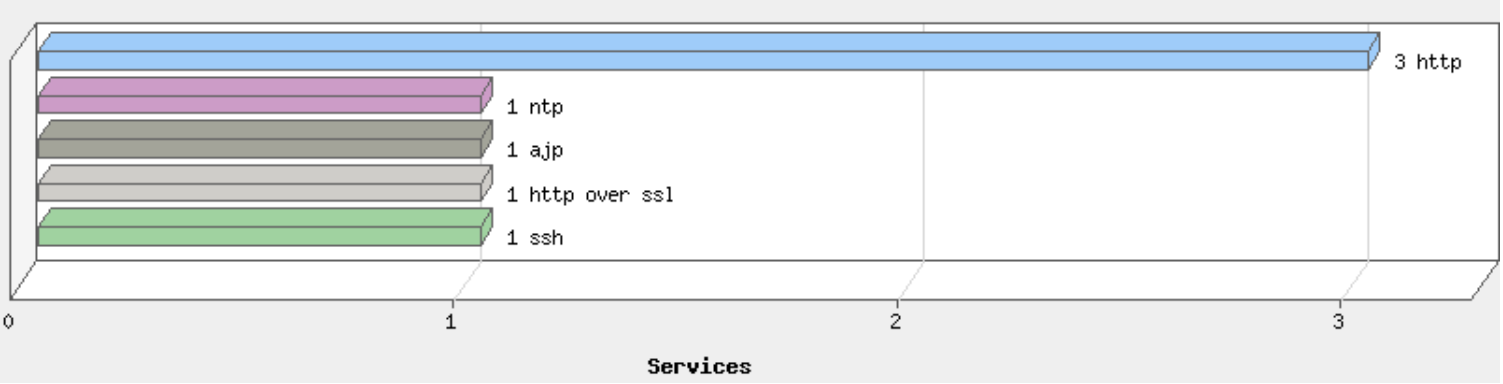
Vulnerabilities by Severity



Operating Systems Detected



Services Detected



Detailed Results

Vulnerabilities (1)

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

QID:	38170
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/12/2015
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

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.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Certificate #0 CN=afm240.tk (afm240.tk) and IP (10.16.133.74) don't match
(www.afm240.tk) and IP (10.16.133.74) don't match
(afm240.tk) and IP (10.16.133.74) don't match

Information Gathered (48)

3 Remote Access or Management Service Detected

QID:	42017
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/03/2016
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

THREAT:
A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks.
The Results section includes information on the remote access service that was found on the target.
Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin), VNC, OPENVPN and ISAKMP are checked.

IMPACT:
Consequences vary by the type of attack.

SOLUTION:
Expose the remote access or remote management services only to the system administrators or intended users of the system.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Service name: SSH on TCP port 22.

 2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/23/2017
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

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 of the firewall instead of 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.

IMPACT:
Not applicable.

SOLUTION:
Not applicable.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
Ubuntu / Fedora / Tiny Core Linux / Linux 3.x	TCP/IP Fingerprint	U5933:22

2 Web Server HTTP Protocol Versions port 80/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Remote Web Server supports HTTP version 1.x on 80 port.GET / HTTP/1.1

2 Web Server Probed For Various URL-Encoding Schemes Supported port 443/tcp

QID:	12059
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/12/2005
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

THREAT:

The target Web server was probed for various URL-encoding schemes that it supports.
Per this paper (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf) 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

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Single-%-Escaped Hex-Encoding Supported

2 Web Server HTTP Protocol Versions — port 443/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 443 port.GET / HTTP/1.1

2 Web Server Probed For Various URL-Encoding Schemes Supported — port 60010/tcp

QID:	12059
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/12/2005
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

THREAT:

The target Web server was probed for various URL-encoding schemes that it supports.
Per this paper (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf) 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

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Single-%-Escaped Hex-Encoding Supported
%-Escaped 2-Byte UTF-8 Encoding Supported
%-Escaped 3-Byte UTF-8 Encoding Supported
Raw 2-Byte UTF-8 Encoding Supported
Raw 3-Byte UTF-8 Encoding Supported

2 Web Server HTTP Protocol Versions — port 60010/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Remote Web Server supports HTTP version 1.x on 60010 port.GET / HTTP/1.1

2 Web Server Probed For Various URL-Encoding Schemes Supported port 60030/tcp

QID:	12059
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/12/2005
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

THREAT:
The target Web server was probed for various URL-encoding schemes that it supports.
Per this paper (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf) 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

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Single-%-Escaped Hex-Encoding Supported
%-Escaped 2-Byte UTF-8 Encoding Supported
%-Escaped 3-Byte UTF-8 Encoding Supported
Raw 2-Byte UTF-8 Encoding Supported
Raw 3-Byte UTF-8 Encoding Supported

2 Web Server HTTP Protocol Versions — port 60030/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 60030 port.GET / HTTP/1.1

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/01/1999
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

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

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
10.16.133.74	No registered hostname

 1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/17/2001
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

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).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Some of the ports filtered by the firewall are: 23.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
23

 1 Traceroute

QID:	45006
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/09/2003
User Modified:	-
Edited:	No

PCI Vuln: No
Ticket State:

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.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Hops	IP	Round Trip Time	Probe
1	10.16.129.254	528.54ms	ICMP
2	10.16.133.74	485.17ms	ICMP

 1 Host Scan Time

QID: 45038
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/19/2016
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

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.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Scan duration: 1528 seconds

Start time: Thu, Apr 27 2017, 05:20:37 GMT

End time: Thu, Apr 27 2017, 05:46:05 GMT

1 UDP Scanning Limited To Default Ports

QID:	45050
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/06/2005
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

THREAT:
Due to the lack of ICMP responses to UDP packets sent to closed ports, the service determined that it was not feasible to scan all UDP ports as requested and limited UDP scanning to the default ports, which consist of about 200 ports that have been found open most frequently in the past. The two most common situations that would cause the service to perform only limited UDP scanning are:
1) The target host was behind a firewall. The service did not receive an ICMP Port Unreachable packet when it sent a UDP packet to a closed port.

2) The target host had a limit on the ICMP transmission rate. For example, the target host only sends at most one ICMP packet per second.

IMPACT:
Some UDP open ports may not have been found open by the service.

SOLUTION:
If possible, do not scan the host through a firewall. If there is a limit on the ICMP transmission rate in the firewall, you may lift the limit for the purposes of scanning.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
No results available

1 Open UDP Services List

QID:	82004
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2005
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

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. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

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. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected
67	bootps	Bootstrap Protocol Server	unknown
123	ntp	Network Time Protocol	ntp
514	syslog	syslog	unknown

1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/16/2009
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

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 (http://www.cert.org).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
22	ssh	SSH Remote Login Protocol	ssh	
80	www	World Wide Web HTTP	http	
443	https	http protocol over TLS/SSL	http over ssl	
2181	unknown	unknown	unknown	
8009	unknown	unknown	AJP	
8989	unknown	unknown	unknown	
60010	unknown	unknown	http	
60030	unknown	unknown	http	

 1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/17/2003
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

THREAT:
ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Unreachable (type=3 code=3)	UDP Port 1	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 20496	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1054	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 137	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 31666	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1011	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1028	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 389	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 407	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 9873	Port Unreachable
Unreachable (type=3 code=2)	IP with High Protocol	Protocol Unreachable

1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/20/2004
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

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

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Average change between subsequent TCP initial sequence numbers is 1515952788 with a standard deviation of 1130134813. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(20771 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/28/2006
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

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

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP ID changes observed (network order) for port 22: 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 0
Duration: 298 milli seconds

1 Host Name Not Available

QID:	82056
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/07/2004
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

THREAT:
Attempts to obtain the fully-qualified domain name (FQDN) or the Netbios name failed for this host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

No results available

1 Apache Tomcat Web Server Running on Target

QID:	86990
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/12/2012
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

THREAT:
Apache Tomcat is an open source web server and servlet container developed by the Apache Software Foundation.
Apache Tomcat is running on this target.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Apache Tomcat webserver running on this host on port: 443
<title>Apache Tomcat/8.0.43 - Error report</title>

1 Unix Authentication Not Attempted

QID:	105297
Category:	Security Policy
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/20/2006
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

THREAT:
Unix authentication was enabled but it was not performed for this particular host because the host's IP address is not included in any Unix authentication records.

IMPACT:
Vulnerabilities that require Unix authentication may not be detected.

SOLUTION:
To allow Unix authentication on this host, include the host's IP address in a Unix authentication record.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
No results available

1 Default Web Page port 443/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/17/2014
User Modified:	-

Edited:	No
PCI Vuln:	No
Ticket State:	

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

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Cache-Control: private
Expires: Wed, 31 Dec 1969 16:00:00 PST
Accept-Ranges: bytes
ETag: W/"105-1493193877000"
Last-Modified: Wed, 26 Apr 2017 08:04:37 GMT
Content-Type: text/html
Content-Length: 105
Date: Thu, 27 Apr 2017 05:26:44 GMT

<html>

<head>
<meta http-equiv="refresh" content="0;URL=/afm">
</head>

<body>
</body>

</html>
```

 1 SSL Server Information Retrieval port 443/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/25/2016
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

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

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM

1 SSL Session Caching Information

port 443/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/16/2004
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

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.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:
TLSv1.2 session caching is enabled on the target.

1 SSL/TLS invalid protocol version tolerance port 443/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/30/2016
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

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 target's 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

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	rejected
0399	rejected
0400	rejected
0499	rejected

1 SSL Certificate will expire within next six months port 443/tcp over SSL

QID:	38600
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/30/2016
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

THREAT:

Certificates are used for authentication purposes in different protocols such as SSL/TLS. Each certificate has a validity period outside of which it is supposed to be considered invalid. This QID is reported to inform that a certificate will expire within next six months. The advance notice can be helpful since obtaining a certificate can take some time.

IMPACT:
Expired certificates can cause connection disruptions or compromise the integrity and privacy of the connections being protected by the certificates.

SOLUTION:
Contact the certificate authority that signed your certificate to arrange for a renewal.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Certificate #0 CN=afm240.tk The certificate will expire within six months: Jul 19 09:13:00 2017 GMT

1 TLS Secure Renegotiation Extension Support Information — port 443/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

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

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLS Secure Renegotiation Extension Status: not supported.

1 SSL Certificate - Information — port 443/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/24/2003
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	03:07:dc:85:7e:c5:a3:c6:55:0b:42:e6:af:23:ee:c0:49:dd
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
organizationName	Let's Encrypt
commonName	Let's Encrypt Authority X3
(0)SUBJECT NAME	
commonName	afm240.tk
(0)Valid From	Apr 20 09:13:00 2017 GMT
(0)Valid Till	Jul 19 09:13:00 2017 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:d0:99:79:0f:28:00:25:87:bf:3a:dd:31:c3:91:
(0)	3e:bf:2e:51:f3:28:bc:86:32:ad:af:31:61:05:28:
(0)	01:d0:da:0f:80:64:dd:b8:d8:53:05:b8:ff:91:55:
(0)	ae:ed:1f:9a:19:46:06:a8:01:47:dd:3d:6b:23:32:
(0)	1c:9b:ac:5f:a1:f7:2b:c8:8c:99:78:cb:24:e6:e3:
(0)	80:8a:27:29:6e:b8:2c:03:e5:d9:97:cd:db:dd:d2:
(0)	70:0e:13:5c:cc:1c:9e:37:c7:c9:da:b1:3e:e4:a7:
(0)	df:3a:48:68:34:56:fa:a9:88:59:f2:32:8d:94:b7:
(0)	4a:93:44:6f:8c:ca:8b:32:55:9d:47:58:d4:62:e0:
(0)	4d:84:b9:0e:03:03:78:6c:09:79:29:a2:a0:e2:56:
(0)	31:3b:0e:86:07:82:83:fe:60:0a:f0:fd:1f:dc:4e:
(0)	c9:d2:c4:28:4a:df:2a:03:91:d5:da:91:ea:36:c8:
(0)	29:c3:f8:01:fe:99:41:7a:ae:36:74:1b:45:85:90:
(0)	7b:b9:fd:25:b4:4f:f1:0a:bd:13:9c:a5:6b:e1:ae:
(0)	3d:92:0b:6a:d4:01:51:1a:a5:54:bc:db:09:05:f9:
(0)	ae:34:ef:42:49:4b:45:21:50:05:a2:f1:60:83:8c:
(0)	0b:62:7f:fa:ee:5b:47:40:f1:6c:c5:4c:03:7c:01:
(0)	a0:81

(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Subject Key Identifier	38:98:FE:18:98:25:A0:A1:F9:1F:CB:11:99:2E:3A:9D:09:31:A8:90
(0)X509v3 Authority Key Identifier	keyid:A8:4A:6A:63:04:7D:DD:BA:E6:D1:39:B7:A6:45:65:EF:F3:A8:EC:A1
(0)Authority Information Access	OCSP - URI:http://ocsp.int-x3.letsencrypt.org/
(0)	CA Issuers - URI:http://cert.int-x3.letsencrypt.org/
(0)X509v3 Subject Alternative Name	DNS:afm240.tk, DNS:www.afm240.tk
(0)X509v3 Certificate Policies	Policy: 2.23.140.1.2.1
(0)	Policy: 1.3.6.1.4.1.44947.1.1.1
(0)	CPS: http://cps.letsencrypt.org
(0)	User Notice:
(0)	Explicit Text: This Certificate may only be relied upon by Relying Parties and only in accordance with the Certificate Policy found at https://letsencrypt.org/repository/
(0)Signature	(256 octets)
(0)	60:9a:37:e0:2a:11:3b:ef:45:1e:ae:ea:c8:2d:2d:73
(0)	ac:79:34:3d:36:f9:90:e8:1b:a4:17:d2:ed:29:bb:54
(0)	34:38:4b:fa:6d:c8:c5:ed:23:62:53:04:0c:ae:fc:56
(0)	c9:40:2d:32:ac:c5:d3:c1:9d:9e:84:aa:15:7e:c1:7f
(0)	47:1b:01:c0:e4:67:43:42:6f:73:0c:0b:b8:2b:c3:1a
(0)	e2:35:29:7b:26:54:6e:32:05:aa:84:77:05:80:14:ae
(0)	0a:c1:8f:8c:8e:0d:c1:ad:aa:d3:96:16:2f:c8:64:20
(0)	e7:0d:c9:9b:b4:8a:37:e3:03:69:ae:48:41:57:fd:bb
(0)	19:20:e2:96:8e:f1:be:6a:a7:bc:5c:79:68:a7:08:29
(0)	0f:c0:69:0f:04:e1:1a:12:6b:a2:26:8c:f9:e2:04:6d
(0)	31:2d:6f:04:a9:c8:62:6e:22:6f:56:c4:7b:3f:4c:dc
(0)	bb:bc:00:b0:66:af:a1:ba:e3:7d:47:f5:f3:53:2d:c1
(0)	04:51:63:fb:c4:d7:3d:0e:7e:8c:88:93:a1:b0:9f:62
(0)	c2:81:9a:4f:b3:2f:e4:50:a2:28:06:2a:08:bf:16:a6
(0)	34:9d:a9:69:13:0f:60:97:57:01:a4:b9:08:6a:e5:d5
(0)	85:71:cb:b0:fa:49:68:d1:8a:70:ba:d3:6b:92:7a:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	0a:01:41:42:00:00:01:53:85:73:6a:0b:85:ec:a7:08
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
organizationName	Digital Signature Trust Co.
commonName	DST Root CA X3
(1)SUBJECT NAME	
countryName	US
organizationName	Let's Encrypt
commonName	Let's Encrypt Authority X3
(1)Valid From	Mar 17 16:40:46 2016 GMT
(1)Valid Till	Mar 17 16:40:46 2021 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:9c:d3:0c:f0:5a:e5:2e:47:b7:72:5d:37:83:b3:
(1)	68:63:30:ea:d7:35:26:19:25:e1:bd:be:35:f1:70:

(1)	92:2f:b7:b8:4b:41:05:ab:a9:9e:35:08:58:ec:b1:
(1)	2a:c4:68:87:0b:a3:e3:75:e4:e6:f3:a7:62:71:ba:
(1)	79:81:60:1f:d7:91:9a:9f:f3:d0:78:67:71:c8:69:
(1)	0e:95:91:cf:fe:e6:99:e9:60:3c:48:cc:7e:ca:4d:
(1)	77:12:24:9d:47:1b:5a:eb:b9:ec:1e:37:00:1c:9c:
(1)	ac:7b:a7:05:ea:ce:4a:eb:bd:41:e5:36:98:b9:cb:
(1)	fd:6d:3c:96:68:df:23:2a:42:90:0c:86:74:67:c8:
(1)	7f:a5:9a:b8:52:61:14:13:3f:65:e9:82:87:cb:db:
(1)	fa:0e:56:f6:86:89:f3:85:3f:97:86:af:b0:dc:1a:
(1)	ef:6b:0d:95:16:7d:c4:2b:a0:65:b2:99:04:36:75:
(1)	80:6b:ac:4a:f3:1b:90:49:78:2f:a2:96:4f:2a:20:
(1)	25:29:04:c6:74:c0:d0:31:cd:8f:31:38:95:16:ba:
(1)	a8:33:b8:43:f1:b1:1f:c3:30:7f:a2:79:31:13:3d:
(1)	2d:36:f8:e3:fc:f2:33:6a:b9:39:31:c5:af:c4:8d:
(1)	0d:1d:64:16:33:aa:fa:84:29:b6:d4:0b:c0:d8:7d:
(1)	c3:93
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE, pathlen:0
(1)X509v3 Key Usage	critical
(1)	Digital Signature, Certificate Sign, CRL Sign
(1)Authority Information Access	OCSP - URI:http://isrg.trustid.ocsp.identrust.com
(1)	CA Issuers - URI:http://apps.identrust.com/roots/dstrootcax3.p7c
(1)X509v3 Authority Key Identifier	keyid:C4:A7:B1:A4:7B:2C:71:FA:DB:E1:4B:90:75:FF:C4:15:60:85:89:10
(1)X509v3 Certificate Policies	Policy: 2.23.140.1.2.1
(1)	Policy: 1.3.6.1.4.1.44947.1.1.1
(1)	CPS: http://cps.root-x1.letsencrypt.org
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.identrust.com/DSTROOTCAX3CRL.crl
(1)X509v3 Subject Key Identifier	A8:4A:6A:63:04:7D:DD:BA:E6:D1:39:B7:A6:45:65:EF:F3:A8:EC:A1
(1)Signature	(256 octets)
(1)	dd:33:d7:11:f3:63:58:38:dd:18:15:fb:09:55:be:76
(1)	56:b9:70:48:a5:69:47:27:7b:c2:24:08:92:f1:5a:1f
(1)	4a:12:29:37:24:74:51:1c:62:68:b8:cd:95:70:67:e5
(1)	f7:a4:bc:4e:28:51:cd:9b:e8:ae:87:9d:ea:d8:ba:5a
(1)	a1:01:9a:dc:f0:dd:6a:1d:6a:d8:3e:57:23:9e:a6:1e
(1)	04:62:9a:ff:d7:05:ca:b7:1f:3f:c0:0a:48:bc:94:b0
(1)	b6:65:62:e0:c1:54:e5:a3:2a:ad:20:c4:e9:e6:bb:dc
(1)	c8:f6:b5:c3:32:a3:98:cc:77:a8:e6:79:65:07:2b:cb
(1)	28:fe:3a:16:52:81:ce:52:0c:2e:5f:83:e8:d5:06:33
(1)	fb:77:6c:ce:40:ea:32:9e:1f:92:5c:41:c1:74:6c:5b
(1)	5d:0a:5f:33:cc:4d:9f:ac:38:f0:2f:7b:2c:62:9d:d9
(1)	a3:91:6f:25:1b:2f:90:b1:19:46:3d:f6:7e:1b:a6:7a
(1)	87:b9:a3:7a:6d:18:fa:25:a5:91:87:15:e0:f2:16:2f
(1)	58:b0:06:2f:2c:68:26:c6:4b:98:cd:da:9f:0c:f9:7f
(1)	90:ed:43:4a:12:44:4e:6f:73:7a:28:ea:a4:aa:6e:7b
(1)	4c:7d:87:dd:e0:c9:02:44:a7:87:af:c3:34:5b:b4:42

1 Default Web Page port 80/tcp

QID: 12230
Category: CGI

CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 06/17/2014
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

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

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Cache-Control: private
Expires: Wed, 31 Dec 1969 16:00:00 PST
Location: https://10.16.133.74/
Content-Length: 0
Date: Thu, 27 Apr 2017 05:23:47 GMT

1 HTTP Methods Returned by OPTIONS Request — port 80/tcp

QID: 45056
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/17/2006
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

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

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Allow: GET, HEAD, POST, PUT, DELETE, OPTIONS

1 Web Server Version port 80/tcp

QID:	86000
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/26/2016
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

THREAT:
N/A

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Server Version	Server Banner
Apache-Coyote/1.1	Apache-Coyote/1.1

1 Apache Web Server Detected port 80/tcp

QID:	86496
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/03/2016
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

THREAT:
Apache, the open source web server software that is developed and maintained by Apache Software Foundation is detected on the host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Apache web server detected on port 80 - Apache-Coyote/1.1

1 Web Server Supports HTTP Request Pipelining port 80/tcp

QID:	86565
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/23/2005
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

THREAT:
Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.
The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:
Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
GET / HTTP/1.1
Host:10.16.133.74:80

GET /Q_Evasive/ HTTP/1.1
Host:10.16.133.74:80

HTTP/1.1 302 Found
Server: Apache-Coyote/1.1

Cache-Control: private
Expires: Wed, 31 Dec 1969 16:00:00 PST
Location: https://10.16.133.74/
Content-Length: 0
Date: Thu, 27 Apr 2017 05:36:42 GMT

HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Cache-Control: private
Expires: Wed, 31 Dec 1969 16:00:00 PST
Location: https://10.16.133.74/Q_Evasive/
Content-Length: 0
Date: Thu, 27 Apr 2017 05:36:42 GMT

1 HTTP Methods Returned by OPTIONS Request — port 443/tcp

QID:	45056
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/17/2006
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

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

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Allow: GET, HEAD, POST, PUT, DELETE, OPTIONS

1 SSL Web Server Version — port 443/tcp

QID:	86001
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/01/1999
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Server Version	Server Banner
Apache-Coyote/1.1	Apache-Coyote/1.1

1 Apache Web Server Detected port 443/tcp

QID:	86496
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/03/2016
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

THREAT:
Apache, the open source web server software that is developed and maintained by Apache Software Foundation is detected on the host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Apache web server detected on port 443 - Apache-Coyote/1.1

1 List of Web Directories port 443/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/11/2004
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

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

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/docs/	web page
/manager/	web page

1 SSH daemon information retrieving port 22/tcp

QID:	38047
Category:	General remote services
CVE ID:	CVE-1999-0634
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/22/2009
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

THREAT:
SSH is a secure protocol, provided it is fully patched, properly configured, and uses FIPS approved algorithms.

For Red Hat ES 4:-
SSH1 supported yes
Supported authentification methods for SSH1 RSA,password
Supported ciphers for SSH1 3des,blowfish
SSH2 supported yes
Supported keys exchange algorithm for SSH2 diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
Supported decryption ciphers for SSH2 aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
Supported encryption ciphers for SSH2 aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
Supported decryption mac for SSH2 hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96
Supported encryption mac for SSH2 hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96
Supported authentification methods for SSH2 publickey,gssapi-with-mic,password

IMPACT:
Successful exploitation allows an attacker to execute arbitrary commands on the SSH server or otherwise subvert an encrypted SSH channel with arbitrary data.

SOLUTION:
SSH version 2 is preferred over SSH version 1.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSH1 supported	no
SSH2 supported	yes
Supported key exchange algorithms for SSH2	curve25519-sha256, curve25519-sha256@libssh.org, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group-exchange-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, diffie-hellman-group14-sha256, diffie-hellman-group14-sha1
Supported host key algorithms for SSH2	ssh-rsa, rsa-sha2-512, rsa-sha2-256
Supported decryption ciphers for SSH2	chacha20-poly1305@openssh.com, aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com, 3des-cbc
Supported encryption ciphers for SSH2	chacha20-poly1305@openssh.com, aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com, 3des-cbc
Supported decryption macs for SSH2	umac-64-etm@openssh.com, umac-128-etm@openssh.com, hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, hmac-sha1-etm@openssh.com, umac-64@openssh.com, umac-128@openssh.com, hmac-sha2-256, hmac-sha2-512, hmac-sha1
Supported encryption macs for SSH2	umac-64-etm@openssh.com, umac-128-etm@openssh.com, hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, hmac-sha1-etm@openssh.com, umac-64@openssh.com, umac-128@openssh.com, hmac-sha2-256, hmac-sha2-512, hmac-sha1
Supported decompression for SSH2	none, zlib@openssh.com
Supported compression for SSH2	none, zlib@openssh.com
Supported authentication methods for SSH2	publickey, password

1 SSH Banner

port 22/tcp

QID:	38050
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/04/2003
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
SSH-2.0-OpenSSH_7.4p1 Debian-10

1 Default Web Page

port 60010/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/17/2014
User Modified:	-
Edited:	No

PCI Vuln: No
Ticket State:

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

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
<!--
/**
 * Licensed to the Apache Software Foundation (ASF) under one
 * or more contributor license agreements.  See the NOTICE file
 * distributed with this work for additional information
 * regarding copyright ownership.  The ASF licenses this file
 * to you under the Apache License, Version 2.0 (the
 * "License"); you may not use this file except in compliance
 * with the License.  You may obtain a copy of the License at
 *
 *     http://www.apache.org/licenses/LICENSE-2.0
 *
 * Unless required by applicable law or agreed to in writing, software
 * distributed under the License is distributed on an "AS IS" BASIS,
 * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
 * See the License for the specific language governing permissions and
 * limitations under the License.
 */
-->
<meta HTTP-EQUIV="REFRESH" content="0;url=/master-status"/>
```

 1 HTTP Methods Returned by OPTIONS Request port 60010/tcp

QID: 45056
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/17/2006
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

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

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Allow: GET, HEAD, POST, TRACE, OPTIONS

1 Web Server Version port 60010/tcp

QID:	86000
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/26/2016
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

THREAT:
N/A

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Server Version	Server Banner
Jetty(6.1.26)	Jetty(6.1.26)

1 Web Server Supports HTTP Request Pipelining port 60010/tcp

QID:	86565
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/23/2005
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

THREAT:
Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.
The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:
Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
GET / HTTP/1.1
Host:10.16.133.74:60010

GET /Q_Evasive/ HTTP/1.1
Host:10.16.133.74:60010

HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
Content-Length: 876
Last-Modified: Tue, 24 Jul 2012 19:30:39 GMT
Server: Jetty(6.1.26)

<!--
/**
 * Licensed to the Apache Software Foundation (ASF) under one
 * or more contributor license agreements. See the NOTICE file
 * distributed with this work for additional information
 * regarding copyright ownership. The ASF licenses this file
 * to you under the Apache License, Version 2.0 (the
 * "License"); you may not use this file except in compliance
 * with the License. You may obtain a copy of the License at
 *
 *   http://www.apache.org/licenses/LICENSE-2.0
 *
 * Unless required by applicable law or agreed to in writing, software
 * distributed under the License is distributed on an "AS IS" BASIS,
 * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
 * See the License for the specific language governing permissions and
 * limitations under the License.
 */
-->
<meta HTTP-EQUIV="REFRESH" content="0;url=/master-status"/>
HTTP/1.1 404 Not Found
Content-Type: text/html; charset=iso-8859-1
Content-Length: 1375
Cache-Control: must-revalidate,no-cache,no-store
Server: Jetty(6.1.26)

<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1"/>
<title>Error 404 NOT_FOUND</title>
</head>
<body><h2>HTTP ERROR 404</h2>
Problem accessing /Q_Evasive/. Reason:
<pre>   NOT_FOUND</pre> <hr /><small>Powered by Jetty://</small>

</body>
</html>

1 Default Web Page port 60030/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/17/2014
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

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

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
<!--
/**
 * Licensed to the Apache Software Foundation (ASF) under one
 * or more contributor license agreements. See the NOTICE file
 * distributed with this work for additional information
 * regarding copyright ownership. The ASF licenses this file
 * to you under the Apache License, Version 2.0 (the
 * "License"); you may not use this file except in compliance
 * with the License. You may obtain a copy of the License at
 *
 *   http://www.apache.org/licenses/LICENSE-2.0
 *
 * Unless required by applicable law or agreed to in writing, software
 * distributed under the License is distributed on an "AS IS" BASIS,

```
 * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
 * See the License for the specific language governing permissions and
 * limitations under the License.
 */
-->
<meta HTTP-EQUIV="REFRESH" content="0;url=/rs-status"/>
```

1 HTTP Methods Returned by OPTIONS Request — port 60030/tcp

QID:	45056
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/17/2006
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

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

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Allow: GET, HEAD, POST, TRACE, OPTIONS

1 Web Server Version — port 60030/tcp

QID:	86000
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/26/2016
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

THREAT:
N/A

IMPACT:
N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Server Version	Server Banner
Jetty(6.1.26)	Jetty(6.1.26)

1 Web Server Supports HTTP Request Pipelining port 60030/tcp

QID:	86565
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/23/2005
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

THREAT:
Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.
The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:
Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.1
Host:10.16.133.74:60030

GET /Q_Evasive/ HTTP/1.1
Host:10.16.133.74:60030

HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Accept-Ranges: bytes
Content-Length: 872
Last-Modified: Tue, 24 Jul 2012 19:30:39 GMT

```
Server: Jetty(6.1.26)

<!--
/**
 * Licensed to the Apache Software Foundation (ASF) under one
 * or more contributor license agreements.  See the NOTICE file
 * distributed with this work for additional information
 * regarding copyright ownership.  The ASF licenses this file
 * to you under the Apache License, Version 2.0 (the
 * "License"); you may not use this file except in compliance
 * with the License.  You may obtain a copy of the License at
 *
 *     http://www.apache.org/licenses/LICENSE-2.0
 *
 * Unless required by applicable law or agreed to in writing, software
 * distributed under the License is distributed on an "AS IS" BASIS,
 * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
 * See the License for the specific language governing permissions and
 * limitations under the License.
 */
-->
<meta HTTP-EQUIV="REFRESH" content="0;url=/rs-status"/>
HTTP/1.1 404 Not Found
Content-Type: text/html; charset=iso-8859-1
Content-Length: 1375
Cache-Control: must-revalidate,no-cache,no-store
Server: Jetty(6.1.26)

<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1"/>
<title>Error 404 NOT_FOUND</title>
</head>
<body><h2>HTTP ERROR 404</h2>
<p>Problem accessing /Q_Evasive/. Reason:
<pre>    NOT_FOUND</pre></p><hr /><i><small>Powered by Jetty://</small></i><br/>
<br/>
<br/>
<br/>
<br/>
<br/>
<br/>
<br/>
<br/>
<br/>
<br/>
<br/>
<br/>
<br/>
<br/>
<br/>
<br/>
<br/>
<br/>
<br/>
<br/>
<br/>
<br/>
<br/>

</body>
</html>
```

Appendix

Hosts Scanned (IP)

10.16.133.74

Target distribution across scanner appliances

ChennaiScanner : 10.16.133.74

Options Profile

d-scan-full-1

Scan Settings

Ports:	
Scanned TCP Ports:	Full
Scanned UDP Ports:	Full
Scan Dead Hosts:	On
Load Balancer Detection:	On
Perform 3-way Handshake:	Off
Vulnerability Detection:	Complete
Include OVAL Checks:	yes
Password Brute Forcing:	
System:	Standard
Custom:	Disabled
Authentication:	
Windows:	Enabled
Unix/Cisco:	Enabled
Oracle:	Enabled
Oracle Listener:	Enabled
SNMP:	Enabled
VMware:	Enabled
DB2:	Disabled
HTTP:	Enabled
MySQL:	Enabled
Overall Performance:	Normal
Authenticated Scan Certificate Discovery:	Enabled
Hosts to Scan in Parallel:	
Use Appliance Parallel ML Scaling:	Off
External Scanners:	15
Scanner Appliances:	30
Processes to Run in Parallel:	
Total Processes:	10
HTTP Processes:	10
Packet (Burst) Delay:	Medium
Port Scanning and Host Discovery:	
Intensity:	Normal
Dissolvable Agent:	
Dissolvable Agent (for this profile):	Disabled
Windows Share Enumeration:	Disabled
Windows Directory Search:	Disabled
Lite OS Discovery:	Enabled

Advanced Settings

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

Report Legend

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.

This report was generated with an evaluation version of Qualys