



L3n

Scan Results

May 04, 2011


Tech Support L3n Ltd
 ntd-tb The Old Telephone Exchange
 Manager 10 Ness Road
 Burwell Cambs, None CB5 0AA
 United Kingdom

Created:05/04/2011 at 14:39:14 (GMT+0100)

Report Summary

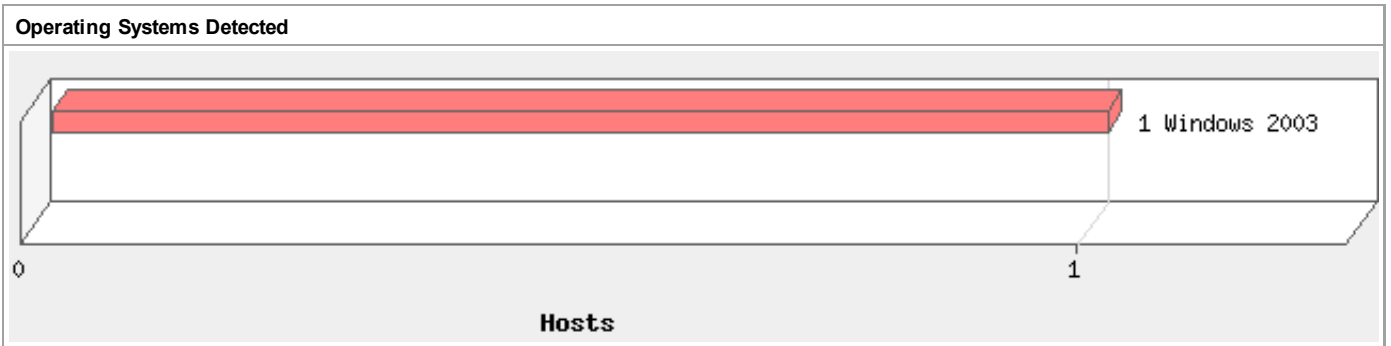
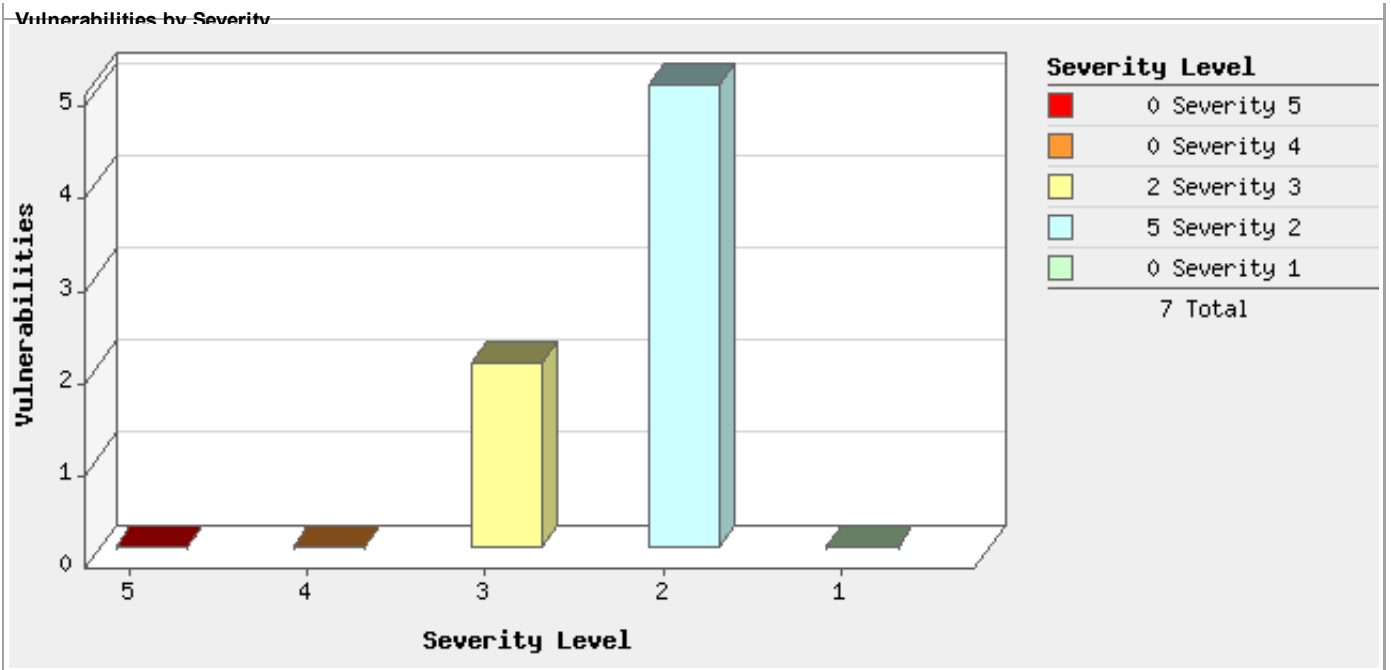
Date: 05/04/2011 at 14:21:04 (GMT+0100)
 Active Hosts: 1
 Total Hosts: 1
 Type: On demand
 Status: Finished
 Reference: scan/1304515264.1698
 Scanner Appliance: x.x.x.x Scanner appliance
 Duration: 00:09:05
 Title: L3n external scan
 Asset Groups: -
 IPs: x.x.x.x
 Option Profile: [Initial Options](#)

Summary of Vulnerabilities

Total: 34 Security Risk (Avg):  3.0

by Severity				
Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	0	0	0	0
3	2	0	0	2
2	5	0	4	9
1	0	0	23	23
Total	7	0	27	34

5 Biggest Categories				
Category	Confirmed	Potential	Information Gathered	Total
Information gathering	0	0	11	11
General remote services	5	0	2	7
Web server	1	0	4	5
Mail services	1	0	4	5
TCP/IP	0	0	4	4
Total	7	0	25	32



Detailed Results

▼ x.x.x.x (abc.co.uk, -)

Windows 2003

▼ Vulnerabilities (7)

▼ 3 SSL Server Has SSLv2 Enabled Vulnerability

port 443/tcp over SSL

QID: 38139
Category: General remote services
CVE ID: -
Vendor Reference: -

Bugtraq ID: -
Service Modified: 07/07/2009
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

The Secure Socket Layer (SSL) protocol allows for secure communication between a client and a server.

There are known flaws in the SSLv2 protocol. A man-in-the-middle attacker can force the communication to a less secure level and then attempt to break the weak encryption. The attacker can also truncate encrypted messages.

These flaws have been fixed in SSLv3 (or TLSv1). Most servers (including all popular Web servers, mail servers, etc.) and clients (including Web-clients like IE, Netscape Navigator and Mozilla and mail clients) support both SSLv2 and SSLv3. However, SSLv2 is enabled by default for backward compatibility.

The following link provides more information about this vulnerability:

[Analysis of the SSL 3.0 Protocol](#)

IMPACT:

An attacker can exploit this vulnerability to read secure communications or maliciously modify messages.

SOLUTION:

Disable SSLv2.

Typically, for Apache/mod_ssl, httpd.conf or ssl.conf should have the following lines:

```
SSLProtocol -ALL +SSLv3 +TLSv1
```

```
SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
```

For Apache/apache_ssl, httpd.conf or ssl.conf should have the following line:

```
SSLNoV2
```

How to disable SSLv2 on IIS : [Microsoft Knowledge Base Article - 187498](#)

How to Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll : [Microsoft Knowledge Base Article - 245030](#)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Established SSLv2 connection using DES-CBC3-MD5 cipher.

▼  3 Mail Server Accepts Plaintext Credentials

port 25/tcp

QID: 74147
Category: Mail services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 05/12/2009
User Modified: -
Edited: No
PCI Vuln: Yes

THREAT:

Your Mail Server responds to the EHLO command which implies that it uses the ESMTP protocol. ESMTP uses the AUTH command which indicates an authentication mechanism to the server. If the server supports the requested authentication mechanism, it performs an authentication protocol exchange to authenticate and identify the user. Optionally, it also negotiates a security layer for subsequent protocol interactions.

Your server accepts PLAIN or LOGIN as one of the AUTH parameters. The authentication credentials are transmitted in plaintext over the network and no encryption is performed.

IMPACT:

Malicious users could obtain mail server credentials by sniffing the traffic. This can allow unauthorized users to use the mail server as an open mail relay. It may also lead to compromise of account credentials that can be used to access other mail services like POP3 and IMAP.

SOLUTION:

Disable the plaintext authentication methods on your SMTP server for unencrypted (non-SSL/TLS) sessions. You may consider using more advanced challenge-based authentication methods like CRAM-MD5 or DIGEST-MD5.

Please contact your vendor for configuration information. Also check [RFC 2554](#) and [RFC 2487](#) for more details.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

EHLO qualysguard.com

```
250-abc.co.uk Hello [64.39.102.71]
250-TURN
250-SIZE
250-ETRN
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-8bitmime
250-BINARYMIME
250-CHUNKING
250-VERFY
250-X-EXPS GSSAPI NTLM LOGIN
250-X-EXPS=LOGIN
250-AUTH GSSAPI NTLM LOGIN
250-AUTH=LOGIN
250-X-LINK2STATE
250-XEXCH50
250 OK
```

▼  2 SSL Certificate - Self-Signed Certificate

port 443/tcp over SSL

QID: 38169
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 05/25/2009
User Modified: -
Edited: No
PCI Vuln: Yes

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 client can trust that the Server Certificate belongs to the server only if it is signed by a mutually trusted third-party Certificate

Authority (CA). Self-signed certificates are created generally for testing purposes or to avoid paying third-party CAs. These should not be used on any production or critical servers.

By exploiting this vulnerability, an attacker can impersonate the server by presenting a fake self-signed certificate. If the client knows that the server does not have a trusted certificate, it will accept this spoofed certificate and communicate with the remote server.

IMPACT:

By exploiting this vulnerability, an attacker can launch a man-in-the-middle attack.

SOLUTION:

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

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 is a self signed certificate.

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

QID: 38170
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 09/29/2008
User Modified: -
Edited: No
PCI Vuln: No

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 QualysGuard 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 (sbs-server.L3n.local) doesn't resolve

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

QID: 38173
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 05/23/2009
User Modified: -
Edited: No
PCI Vuln: Yes

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.

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 self signed certificate

▼  2 Pre-shared Key Off-line Bruteforcing Using IKE Aggressive Mode port 500/udp

QID: 38498
Category: General remote services
CVE ID: -
Vendor Reference: [cisco-sn-20030422-ike](#)
Bugtraq ID: -
Service Modified: 05/22/2008
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

IKE is used during Phase 1 and Phase 2 of establishing an IPsec connection. Phase 1 is where the two ISAKMP peers

establish a secure, authenticated channel with which to communicate. Every participant in IKE must possess a key which may be either pre-shared (PSK) or a public key. There are inherent risks to configurations that use pre-shared keys which are exaggerated when Aggressive Mode is used.

IMPACT:

Using Aggressive Mode with pre-shared keys is the least secure option. In this particular scenario, it is possible for an attacker to gather all necessary information in order to mount an off-line dictionary (brute force) attack on the pre-shared keys. For more information about this type of attack, visit <http://www.ernw.de/download/pskattack.pdf>.

SOLUTION:

IKE Aggressive mode with pre-shared keys should be avoided where possible. Otherwise a strong pre-shared key should be chosen.

Note that this attack method has been known and discussed within the IETF IPsec Working Group. The risk was considered as acceptable. For more information on this, visit http://www.vpnc.org/ietf-ipsec/99_ipsec/thrd2.htm#01451.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:


There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

37ee5059e4211128704139a12e036820

▼  2 Web Server Internal IP Address/Internal Network Name Disclosure Vulnerability port 443/tcp

QID: 86247
Category: Web server
CVE ID: [CVE-2000-0649](#)
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/02/2008
User Modified: -
Edited: No
PCI Vuln: No

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.

Workarounds:

For IIS Web Server:

Check the Microsoft article on [how to set the Hostname instead of internal IP address for IIS](#).

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.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET /exchange/ HTTP/1.0

HTTP/1.1 302 Moved Temporarily

Location: https://192.168.200.10/exchweb/bin/auth/owalogon.asp?url=https://192.168.200.10/exchange/&reason=0

Set-Cookie: sessionid=; path=/; expires=Thu, 01-Jan-1970 00:00:00 GMT

Set-Cookie: cadata=; path=/; expires=Thu, 01-Jan-1970 00:00:00 GMT

Connection: close

Content-Length: 0

▼ Information Gathered (27) **▼**  **2 Operating System Detected**

QID: 45017

Category: Information gathering

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Service Modified: 02/09/2005

User Modified: -

Edited: No

PCI Vuln: No

THREAT:

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

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

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

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

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

4) **SNMP:** The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach.

The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB-II.system.sysDescr" for the operating system.

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
Windows 2003	TCP/IP Fingerprint	U1752:25

▼  2 SMTP Banner port 25/tcp

QID: 74042
Category: Mail services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/11/2003
User Modified: -
Edited: No
PCI Vuln: No

SOLUTION:

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

220 abc.co.uk Microsoft ESMTP MAIL Service, Version: 6.0.3790.4675 ready at Wed, 4 May 2011 14:21:56 +0100

▼  2 SMTP Service Detected port 25/tcp

QID: 74145
Category: Mail services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 09/20/2004
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The Mail Service on this host can be identified from a remote system using SMTP fingerprinting. According to the results of this fingerprinting technique the Mail Service name and version are listed below

the fingerprint technique, the mail service name and version are listed below.

SOLUTION:

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Name: Microsoft ESMTP MAIL Service, Version: 6.0.3790.4675

▼  2 IMAP Banner port 143/tcp

QID: 50010
Category: Mail services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/01/1999
User Modified: -
Edited: No
PCI Vuln: No

SOLUTION:

COMPLIANCE:

Not Applicable

EXPLOITABILITY:


There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

* OK Microsoft Exchange Server 2003 IMAP4rev1 server version 6.5.7638.1 (sbs-server.L3n.local) ready.

▼  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

THREAT:

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

SOLUTION:

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
x.x.x.x	abc.co.uk

▼  1 Firewall Detected

QID: 34011
Category: Firewall
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 10/16/2001
User Modified: -
Edited: No
PCI Vuln: No

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).

SOLUTION:**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: 20, 21, 22, 23, 53, 80, 111, 135, 445, 1.

▼  1 Target Network Information

QID: 45004
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 11/10/2003
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

This information was gathered using WHOIS service for the target network. Note that this is not all the information that WHOIS service provides.

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:**COMPLIANCE:**

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

The network handle is: KEME-DSL-77dbc1cd09f3ec8d

Network description:

KeConnect DSL Customer

▼  1 Internet Service Provider

QID: 45005
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 11/10/2003
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

This information was gathered using the WHOIS service for the network and is believed to be the ISP of the target network.

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:

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

The ISP network handle is: KEME-ADSLPOOL-3

ISP Network description:

Single Static IP Addresses

▼  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

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.

SOLUTION:

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	x.x.x.x	0.19ms	ICMP
2	89.202.187.217	0.32ms	ICMP
3	84.233.208.50	15.62ms	ICMP
4	84.233.208.17	15.64ms	ICMP
5	84.233.208.25	15.81ms	ICMP
6	212.23.42.25	9.10ms	ICMP
7	212.23.42.22	15.47ms	ICMP
8	195.66.224.111	15.95ms	ICMP
9	x.x.x.x	15.91ms	ICMP
10	x.x.x.x	35.33ms	ICMP
11	x.x.x.x	38.19ms	TCP

▼  1 Virtual Private Networks

QID: 45013
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/01/1999
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

This host allows Virtual Private Network connections to be established from remote VPN clients.

SOLUTION:**COMPLIANCE:**

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	Service	Description
1723	PPTP	Point-To-Point Tunneling Protocol
500	ISAKMP/IKE	ISAKMP/IKE key exchange for IPsec Virtual Private Network

▼  1 VPN Authentications

QID: 45014
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -

Service Modified: 11/10/2003

User Modified: -

Edited: No

PCI Vuln: No

THREAT:

The following authentication policies are supported by the VPN servers on this host:

SOLUTION:

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Authentication	Description
Preshared Key	Client and server share a secret, preconfigured key.

▼  1 IKE Service Implementation Identified

QID: 45018

Category: Information gathering

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Service Modified: 12/23/2003

User Modified: -

Edited: No

PCI Vuln: No

THREAT:

The IKE service implementation active on this host can be identified from a remote system using IKE fingerprinting. All IKE service implementations have subtle differences that can be seen in their responses to specially crafted packets. According to the results of this "fingerprinting" technique, the IKE service implementation is among those listed below.

If one or more of these subtle differences is modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the IKE implementation may not be detected correctly.

IMPACT:

Through acquired knowledge of the IKE implementation, an attacker can launch further attacks against the service or try to bypass it.

SOLUTION:

COMPLIANCE:

Not Applicable

EXPLOITABILITY:


There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Cisco PIX Firewall/VPN Concentrator

▼  1 Host Scan Time

QID: 45038

Category: Information gathering
CVE ID: -
Vendor Reference -
Bugtraq ID: -
Service Modified: 11/19/2004
User Modified: -
Edited: No
PCI Vuln: No

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

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: 493 seconds

Start time: Wed, May 04 2011, 13:21:04 GMT

End time: Wed, May 04 2011, 13:29:17 GMT

▼  1 Host Names Found

QID: 45039
Category: Information gathering
CVE ID: -
Vendor Reference -
Bugtraq ID: -
Service Modified: 02/14/2005
User Modified: -
Edited: No
PCI Vuln: No

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

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
abc.co.uk	FQDN

▼  1 Open UDP Services List

QID: 82004
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/11/2005
User Modified: -
Edited: No
PCI Vuln: No

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](#).

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
500	isakmp	isakmp	isakmp

▼  1 Open TCP Services List

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

Bugtraq ID: -
Service Modified: 06/15/2009
User Modified: -
Edited: No
PCI Vuln: No

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](#).

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
25	smtp	Simple Mail Transfer	smtp	
143	imap	Internet Message Access Protocol	imap	
443	https	http protocol over TLS/SSL	http over ssl	
1723	pptp	pptp	pptp	

▼  1 Degree of Randomness of TCP Initial Sequence Numbers

QID: 82045
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 11/19/2004
User Modified: -
Edited: No
PCI Vuln: No

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:

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:

Content-Length: 1549
 Content-Type: text/html
 Server: Microsoft-IIS/6.0
 MicrosoftOfficeWebServer: 5.0_Pub
 X-Powered-By: ASP.NET
 Date: Wed, 04 May 2011 13:21:57 GMT
 Connection: close

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>You are not authorized to view this page</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=Windows-1252">
<STYLE type="text/css">
BODY { font: 8pt/12pt verdana }
H1 { font: 13pt/15pt verdana }
H2 { font: 8pt/12pt verdana }
A:link { color: red }
A:visited { color: maroon }
</STYLE>
</HEAD><BODY><TABLE width=500 border=0 cellspacing=10><TR><TD>
```

<h1>You are not authorized to view this page</h1>

The Web server you are attempting to reach has a list of IP addresses that are not allowed to access the Web site, and the IP address of your browsing computer is on this list.

<hr>

<p>Please try the following:</p>

Contact the Web site administrator

▼  1 SSL Server Information Retrieval

port 443/tcp over SSL

QID: 38116
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/29/2005
User Modified: -
Edited: No
PCI Vuln: No

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 that allow connections to be established using a

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 ENABLED					
DES-CBC3-MD5	RSA	RSA	MD5	3DES(168)	HIGH
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC2-CBC-MD5	RSA	RSA	MD5	RC2(128)	MEDIUM
EXP-RC4-MD5	RSA(512)	RSA	MD5	RC4(40)	LOW
EXP-RC2-CBC-MD5	RSA(512)	RSA	MD5	RC2(40)	LOW
DES-CBC-MD5	RSA	RSA	MD5	DES(56)	LOW
SSLv3 PROTOCOL IS ENABLED					
DES-CBC3-MD5	RSA	RSA	MD5	3DES(168)	HIGH
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC2-CBC-MD5	RSA	RSA	MD5	RC2(128)	MEDIUM
EXP-RC4-MD5	RSA(512)	RSA	MD5	RC4(40)	LOW
EXP-RC2-CBC-MD5	RSA(512)	RSA	MD5	RC2(40)	LOW
DES-CBC-MD5	RSA	RSA	MD5	DES(56)	LOW
EXP1024-RC4-SHA	RSA(1024)	RSA	SHA1	RC4(56)	LOW
EXP1024-DES-CBC-SHA	RSA(1024)	RSA	SHA1	DES(56)	LOW
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	HIGH
DES-CBC-SHA	RSA	RSA	SHA1	DES(56)	LOW
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
TLSv1 PROTOCOL IS ENABLED					
DES-CBC3-MD5	RSA	RSA	MD5	3DES(168)	HIGH
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC2-CBC-MD5	RSA	RSA	MD5	RC2(128)	MEDIUM
EXP-RC4-MD5	RSA(512)	RSA	MD5	RC4(40)	LOW
EXP-RC2-CBC-MD5	RSA(512)	RSA	MD5	RC2(40)	LOW
DES-CBC-MD5	RSA	RSA	MD5	DES(56)	LOW
EXP1024-RC4-SHA	RSA(1024)	RSA	SHA1	RC4(56)	LOW
EXP1024-DES-CBC-SHA	RSA(1024)	RSA	SHA1	DES(56)	LOW
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	HIGH
DES-CBC-SHA	RSA	RSA	SHA1	DES(56)	LOW

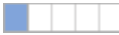
RC4-SHA

RSA

RSA

SHA1 RC4(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

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:**COMPLIANCE:**

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSLv3 session caching is enabled on the target. TLSv1 session caching is enabled on the target.

▼  1 Microsoft Exchange Server Version Detected

port 443/tcp over SSL

QID: 74166
Category: Mail services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/18/2011
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The Microsoft Exchange Server version installed on this host was detected.

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:

Microsoft Office Outlook Web Access provided by Microsoft Exchange Server 2003"

▼  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

SOLUTION:

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	(Negative) 3f:31:89:b6:3d:58:39:72:bd:6b:dc:b3:51:97:6e:f0
(0)Signature Algorithm	sha1WithRSAEncryption
(0)ISSUER NAME	
commonName	sbs-server.L3n.local
commonName	localhost
commonName	sbs-server
commonName	companyweb
commonName	abc.co.uk
(0)SUBJECT NAME	
commonName	sbs-server.L3n.local
commonName	localhost
commonName	sbs-server
commonName	companyweb
commonName	abc.co.uk
(0)Valid From	Jun 8 15:54:43 2007 GMT
(0)Valid Till	Jun 8 15:54:43 2012 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(1024 bit)
(0)	Modulus (1024 bit):
(0)	00:de:7e:15:44:2f:99:60:f1:20:55:92:26:72:d6:
(0)	84:b6:a8:b2:08:d9:27:6a:58:56:7c:90:e7:37:dd:
(0)	83:f2:7f:a2:d7:20:03:3e:56:01:8c:2b:36:58:ea:

(0) dd:d8:7f:09:5d:6c:6b:2e:02:ed:71:88:4d:e0:16:
 (0) 73:da:35:8e:01:8a:3d:9f:30:8b:9d:83:6b:90:ef:
 (0) d6:46:c9:cb:a8:60:d1:5a:96:cd:6f:a2:07:0c:be:
 (0) ca:69:19:19:97:49:13:3b:2a:7c:2d:40:21:a1:63:
 (0) 9c:f5:fa:0e:8d:f2:d1:d0:dd:a9:c6:a1:c1:da:d9:
 (0) 23:aa:f1:24:34:a9:c2:1b:1d
 (0) Exponent: 65537 (0x10001)
 (0)Signature (128 octets)
 (0) 6f:de:f1:99:79:98:b8:7d:ca:c3:02:72:ec:b7:99:e7
 (0) 80:f2:60:74:02:63:5c:4b:ef:92:cd:0e:cf:18:9e:f3
 (0) e0:70:a1:7a:f9:71:90:6f:fa:51:c9:62:ba:de:f5:fc
 (0) f9:d4:c9:22:b1:ff:d5:62:ab:83:38:fb:37:3e:fd:49
 (0) 7b:8d:e3:25:e3:6b:c6:65:b8:0b:80:61:eb:14:98:6f
 (0) 78:ce:e9:07:0f:0e:ac:c1:75:d3:42:e0:bb:76:12:5a
 (0) 81:8a:1e:c3:f2:f8:f6:52:e7:54:d4:b7:b0:27:ac:a2
 (0) 61:3a:be:a0:25:77:0d:1b:31:d1:99:32:c0:0e:8c:a3

▼  1 Web Server Supports HTTP Request Pipelining

port 443/tcp over SSL

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

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](#), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Splitting 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:x.x.x.x:443

GET /Q_Evasive/ HTTP/1.1

Host: x.x.x.x:443

HTTP/1.1 403 Forbidden
Content-Length: 1549
Content-Type: text/html
Server: Microsoft-IIS/6.0
MicrosoftOfficeWebServer: 5.0_Pub
X-Powered-By: ASP.NET
Date: Wed, 04 May 2011 13:22:14 GMT

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>You are not authorized to view this page</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=Windows-1252">
<STYLE type="text/css">
BODY { font: 8pt/12pt verdana }
H1 { font: 13pt/15pt verdana }
H2 { font: 8pt/12pt verdana }
A:link { color: red }
A:visited { color: maroon }
</STYLE>
</HEAD><BODY><TABLE width=500 border=0 cellspacing=10><TR><TD>
```

```
<h1>You are not authorized to view this page</h1>
The Web server you are attempting to reach has a list of IP addresses that are not allowed to access the Web site, and the IP
address of your browsing computer is on this list.
<hr>
<p>Please try the following:</p>
<ul>
<li>Contact the Web site administrator if you believe you should be able to view this directory or page.</li>
</ul>
<h2>HTTP Error 403.6 - Forbidden: IP address of the client has been rejected.<br>Internet Information Services (IIS)</h2>
<hr>
<p>Technical Information (for support personnel)</p>
<ul>
<li>Go to <a href="http://go.microsoft.com/fwlink/?linkid=8180">Microsoft Product Support Services</a> and perform a title
search for the words <b>HTTP</b> and <b>403</b>.</li>
<li>Open <b>IIS Help</b>, which is accessible in IIS Manager (inetmgr),
and search for topics titled <b>About Security</b>, <b>Limiting Access by IP Address</b>, <b>IP Address Access
Restrictions</b>, and <b>About Custom Error Messages</b>.</li>
</ul>
```

```
</TD></TR></TABLE></BODY></HTML>
HTTP/1.1 403 Forbidden
Content-Length: 1549
Content-Type: text/html
Server: Microsoft-IIS/6.0
MicrosoftOfficeWebServer: 5.0_Pub
X-Powered-By: ASP.NET
Date: Wed, 04 May 2011 13:22:14 GMT
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>You are not authorized to view this page</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=Windows-1252">
<STYLE type="text/css">
BODY { font: 8pt/12pt verdana }
H1 { font: 13pt/15pt verdana }
H2 { font: 8pt/12pt verdana }
A:link { color: red }
A:visited { color: maroon }
</STYLE>
```

</HEAD><BODY><TABLE width=500 border=0 cellspacing=10><TR><TD>

<h1>You are not authorized to view this page</h1>

The Web server you are attempting to reach has a list of IP addresses that are not allowed to access the Web site, and the IP address of your browsing computer is on this list.

<hr>

<p>Please try the following:</p>

Contact the Web site administrator if you believe you should be able to view this directory or page.

<h2>HTTP Error 403.6 - Forbidden: IP address of the client has been rejected.
Internet Information Services (IIS)</h2>

<hr>

<p>Technical Information (for support personnel)</p>

Go to Microsoft Product Support Services and perform a title search for the words HTTP and 403.

Open IIS Help, which is accessible in IIS Manager (inetmgr), and search for topics titled About Security, Limiting Access by IP Address, IP Address Access Restrictions, and About Custom Error Messages.

</TD></TR></TABLE></BODY></HTML>

▼  1 Microsoft IIS Server Detected port 443/tcp

QID: 45104
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/13/2009
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Microsoft Internet Information Services (IIS) Web Server was detected on the target 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:

Microsoft-IIS/6.0

▼  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

SOLUTION:

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
Microsoft-IIS/6.0	Microsoft-IIS/6.0

▼  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

THREAT:

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

SOLUTION:

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
/exchweb/	web page
/exchweb/img/	web page

▼ Appendix

Hosts Scanned

Successfully Scanned Hosts

x.x.x.x

Target distribution across scanner appliances

External : x.x.x.x

Options Profile

Initial Options

Scan Settings

Ports	-
Scanned TCP Ports	Standard Scan
Scanned UDP Ports	Standard Scan
Scan Dead Hosts	Off
Load Balancer Detection	Off
Perform 3-way Handshake	Off
Vulnerability Detection	Complete
Password Brute Forcing	-
System	Disabled
Custom	Disabled
Authentication	-
Windows	Disabled
Unix/Cisco IOS	Disabled
Oracle	Disabled
Oracle Listener	Disabled
SNMP	Disabled
Overall Performance	Normal
Hosts to Scan in Parallel	-
External Scanners	15
Scanner Appliances	30
Processes to Run in Parallel	-
Total	10
HTTP	10
Packet (Burst) Delay	Medium
Port Scanning and Host Discovery	-
Intensity	Normal

Advanced Settings

Host Discovery	TCP Standard Scan
	UDP Standard Scan
	ICMP On
Packet Options	-
Ignore firewall-generated TCP RST packets	Off
Ignore all TCP RST packets	Off

Ignore all TCP RST packets

On

Ignore firewall-generated TCP SYN-ACK packets

Off






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.



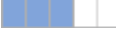
Severity	Level	Description
	1 Minimal	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
	2 Medium	If this vulnerability exists on your system, intruders may 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.

CONFIDENTIAL AND PROPRIETARY INFORMATION. Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2011, Qualys, Inc.
