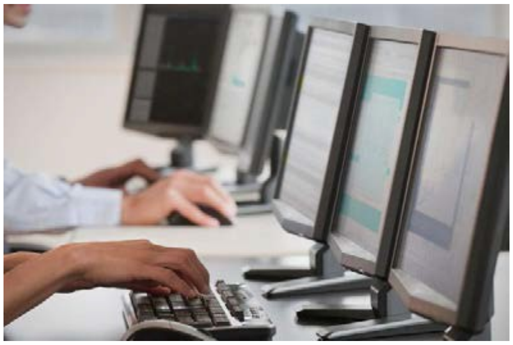
Vulnerability Report for 2015

XYZ Computer Company



Prepared By

ITMS, LLC
Is Your Information Safe From Prying Eyes?
Kenneth C. Romer Certified Ethical Hacker
We Specialize In Network Security Scans.
855 369 4867
kcr@itms.us.com / www.itms.us.com

Executive Summary

This document details the results of a security test conducted by the ITMS testing team in January 2015 remotely from an ITMS facility. The purpose of this engagement was to perform a vulnerability scan of Eight (8) systems used by XYZ Company. The objectives of this engagement were to:

- Perform a vulnerability scan of up to Eight (8) externally accessible systems
- Log all actions taken and data collected during the testing process
- Create a report documenting all testing actions, findings, and recommendations for corrective actions

Overall these systems can be improved by implementing the following recommendations and by addressing all the priorities described in this report.

Findings and Recommendations

During the course of this engagement, ITMS identified several issues with server configurations. ITMS found a few **Medium** issues on several systems. Refer to the report documentation to identify issues to systems. Any findings not noted here are low or informational only.

Backup Files Disclosure. - It is possible to retrieve file backups from the remote web server.

Solution
Ensure the files do not contain any sensitive information, such as credentials to connect to a database, and delete or protect those files that should not be accessible.

SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability. - It may be possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

Solution
Configure SSL/TLS servers to only use TLS 1.1 or TLS 1.2 if supported.
Configure SSL/TLS servers to only support cipher suites that do not use block ciphers. Apply patches if available.
Note that additional configuration may be required after the installation of the MS12-006 security update in order to enable the split-record countermeasure. See Microsoft KB2643584 for details.

SSL Anonymous Cipher Suites Supported. - The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.

Solution
Reconfigure the affected application if possible to avoid use of weak ciphers.

TLS CRIME Vulnerability. - The remote service has a configuration that may make it vulnerable to the CRIME attack.

Solution
Disable compression and / or the SPDY service.

Test Methodology

External Vulnerability Scanning

After the set of Internet accessible addresses is defined, ITMS will meet with Customer to determine which addresses will be included in the full vulnerability scan. Vulnerability scanning identifies information about the operating system, network services, applications, and versions of those items that are active on targeted systems. After the configuration of the systems and networks is defined in more detail, exploitable vulnerabilities known to exist in those configurations are identified and documented. In addition, data collected by the tools may allow the test team to identify operating systems in use on those systems, and network service applications that are available (SMTP, DNS, HTTP, etc). External scanning (i.e. performed across the Internet) will reveal the services that are available on targeted systems from outside the Customer environment. Any vulnerabilities will be identified and documented, but will not be exploited by the ITMS team.

The next phase of the vulnerability scanning process utilizes medium intensity probes to identify the versions of service applications that are in use. Identification of service application version information is useful because many vulnerabilities contained in network applications are version specific, and knowing the version number allows specific problems to be targeted. ITMS will develop a report that recaps the vulnerability scanning process and identifies the prioritized security findings and risks with risk mitigating recommendations. The vulnerabilities and risks levels are clearly listed for the overall test, and by system. The report also includes a listing of each active system identified during the scan, and all vulnerabilities that may be found on each system. Each vulnerability listing includes a description and recommendation for corrective action.

A full vulnerability scanning report will be delivered for the entire set of systems that were included in the vulnerability scan. ITMS will develop a report that recaps the assessment process and identifies the prioritized security findings and risks with risk mitigating recommendations.

OWASP

Tenable can be found on the home page of the OWASP as a corporate supporter.

ITMS utilizes ITMS Professional Feed as its primary scanning tool. This tool was developed by Tenable Network Security. Tenable Network Security is a proud sponsor of the Open Web Application Security Project (OWASP) and has specifically added technology and checks to the ITMS vulnerability scanner to make it easier to find risks identified by this project.

OWASP first published web application audit guidelines in 2004. OWASP guidelines are labeled as risks A1 through A10.

ITMS provides unredacted Raw Web application Penetration Test Results that are aligned with the OWASP model.

We test for the following during an external vulnerability scan:

CGI abuses – This plug-in family checks for a wide range of commercial and open source applications that have documented vulnerabilities. These checks include software detection, information disclosure, SQL injection, file inclusion, overflows and more.

CGI abuses : XSS – This plug-in family checks for a wide range of commercial and open source applications that have documented Cross-site Scripting (XSS) vulnerabilities

General – This plug-in family contains plug-ins that identifies operating systems via HTTP; perform a wide variety of SSL checks and more.

Service detection – Contains checks for a wide variety of services and technologies, many of which support web servers and applications.

Web servers – This plug-in family contains over 500 checks for vulnerabilities in popular web servers including Apache, Tomcat, IIS and WebSphere. In addition, this plug-in family includes checks for frameworks such as PHP, common web server issues associated with the HTTP(S) protocol, OpenSSL checks and more.

000.000.000.000

Summary

Critical	High	Medium	Low	Info	Total
0	0	3	0	27	30

Details

Severity	Plugin Id	Name
Medium (5.0)	11411	Backup Files Disclosure
Medium (4.3)	58751	SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability
Medium (4.3)	62565	TLS CRIME Vulnerability
Info	10107	HTTP Server Type and Version
Info	10267	SSH Server Type and Version Information
Info	10287	Traceroute Information
Info	10302	Web Server robots.txt Information Disclosure
Info	10662	Web mirroring
Info	10863	SSL Certificate Information
Info	11032	Web Server Directory Enumeration
Info	11219	ITMS SYN scanner
Info	11935	IPSEC Internet Key Exchange (IKE) Version 1 Detection
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	39463	HTTP Server Cookies Set
Info	39520	Backported Security Patch Detection (SSH)
Info	42057	Web Server Allows Password Auto-Completion
Info	43111	HTTP Methods Allowed (per directory)
Info	45590	Common Platform Enumeration (CPE)
Info	46180	Additional DNS Hostnames
Info	49704	External URLs
Info	49705	Web Server Harvested Email Addresses
Info	50845	OpenSSL Detection

Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62563	SSL Compression Methods Supported

Scan Information

Host Information

DNS Name:	-static.hfc.comcastbusiness.net
IP:	xxxxxxxxx
OS:	Microsoft Windows Vista

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	5	0	32	37

Results Details

0/tcp

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

ITMS was able to resolve the FQDN of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2004/02/11, Modification date: 2012/09/28

Ports

tcp/0

```
-static.hfc.comcastbusiness.net.
```

46180 - Additional DNS Hostnames

Synopsis

Potential virtual hosts have been detected.

Description

Hostnames different from the current hostname have been collected by miscellaneous plugins. Different web servers may be hosted on name- based virtual hosts.

See Also

http://en.wikipedia.org/wiki/Virtual_hosting

Solution

If you want to test them, re-scan using the special vhost syntax, such as :
www.example.com[192.0.32.10]

Risk Factor

None

Plugin Information:

Publication date: 2010/04/29, Modification date: 2011/06/22

Ports

tcp/0

```
-
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes, (TCP/IP, SMB, HTTP, NTP, SNMP, etc...) it is possible to guess the name of the remote operating system in use, and sometimes its version.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2003/12/09, Modification date: 2012/12/01

Ports

tcp/0

```
Remote operating system : Microsoft Windows Vista
Confidence Level : 65
Method : SinFP


The remote host is running Microsoft Windows Vista
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/05/23, Modification date: 2011/05/23

Ports

tcp/0

```
Remote device type : general-purpose
Confidence level : 65
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It is possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a ITMS scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.
Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2013/01/17

Ports

tcp/0

```
The remote operating system matched the following CPE :

  cpe:/o:microsoft:windows_vista

Following application CPE matched on the remote system :

  cpe:/a:openbsd:openssh:5.4 -> OpenBSD  OpenSSH 5.4
```

0/udp

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2012/02/23

Ports

udp/0

```
For your information, here is the traceroute from 192.168.1.2 to xxx.xxx.xxx.xxx :
192.168.1.2
192.168.1.1
98.110.91.1
130.81.216.6
130.81.209.140
130.81.23.194
130.81.17.121
152.63.18.73
209.58.26.93
209.58.26.86
xx.86.87xxxx
```

22/tcp

11219 - ITMS SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner.
It shall be reasonably quick even against a firewalled target.
Note that SYN scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Ports

tcp/22

```
Port 22/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2012/11/20

Ports

tcp/22

```
An SSH server is running on this port.
```

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2011/10/24

Ports

tcp/22

```

SSH version : SSH-2.0-OpenSSH_5.4
```

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.
Banner-based checks have been disabled to avoid false positives.
Note that this test is informational only and does not denote any security problem.

See Also

http://www.ITMS.org/u?d636c8c7

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2009/06/25, Modification date: 2012/02/02

Ports

tcp/22

```
Give ITMS credentials to perform local checks.
```

80/tcp

11219 - ITMS SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner.
It shall be reasonably quick even against a firewalled target.
Note that SYN scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Ports

tcp/80

```
Port 80/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2012/11/20

Ports

tcp/80

```
A web server is running on this port.
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/01/04, Modification date: 2012/08/02

Ports

tcp/80

```
The remote web server type is :

SonicWALL
```

443/tcp

58751 - SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability

Synopsis

It may be possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

Description

A vulnerability exists in SSL 3.0 and TLS 1.0 that could allow information disclosure if an attacker intercepts encrypted traffic served from an affected system.
TLS 1.1, TLS 1.2, and all cipher suites that do not use CBC mode are not affected.
This script tries to establish an SSL/TLS remote connection using an affected SSL version and cipher suite, and then solicits return data.
If returned application data is not fragmented with an empty or one-byte record, it is likely vulnerable.
OpenSSL uses empty fragments as a countermeasure unless the 'SSL_OP_DONT_INSERT_EMPTY_FRAGMENTS' option is specified when OpenSSL is initialized.
Microsoft implemented one-byte fragments as a countermeasure, and the setting can be controlled via the registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\SendExtraRecord.
Therefore, if multiple applications use the same SSL/TLS implementation, some may be vulnerable while others may not, depending on whether or not a countermeasure has been enabled.
Note that this script detects the vulnerability in the SSLv3/TLSv1 protocol implemented in the server. It does not detect the BEAST attack where it exploits the vulnerability at HTTPS client-side (i.e., Internet browser). The detection at server-side does not necessarily mean your server is vulnerable to the BEAST attack because the attack exploits the vulnerability at client-side, and both SSL/TLS clients and servers can independently employ the split record countermeasure.

See Also

http://www.openssl.org/~bodo/tls-cbc.txt

http://vnhacker.blogspot.com/2011/09/beast.html

http://technet.microsoft.com/en-us/security/bulletin/ms12-006

http://support.microsoft.com/kb/2643584

http://blogs.msdn.com/b/kaushal/archive/2012/01/21/fixing-the-beast.aspx

Solution

Configure SSL/TLS servers to only use TLS 1.1 or TLS 1.2 if supported.
Configure SSL/TLS servers to only support cipher suites that do not use block ciphers. Apply patches if available.
Note that additional configuration may be required after the installation of the MS12-006 security update in order to enable the split-record countermeasure. See http://support.microsoft.com/kb/2643584 for details.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.6 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

STIG Severity

I

References

BID	49778

CVE	CVE-2011-3389
XREF	OSVDB:74829
XREF	MSFT:MS12-006
XREF	IAVB:2012-B-0006

Plugin Information:

Publication date: 2012/04/16, Modification date: 2012/10/23

Ports

tcp/443

```
Negotiated cipher suite: AES256-SHA|TLSv1|Kx=RSA|Au=RSA|Enc=AES(256)|Mac=SHA1
```

20007 - SSL Version 2 (v2) Protocol Detection

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

Description

The remote service accepts connections encrypted using SSL 2.0, which reportedly suffers from several cryptographic flaws and has been deprecated for several years. An attacker may be able to exploit these issues to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients.

See Also

http://www.schneier.com/paper-ssl.pdf

http://support.microsoft.com/kb/187498

http://www.linux4beginners.info/node/disable-sslv2

Solution

Consult the application's documentation to disable SSL 2.0 and use SSL 3.0, TLS 1.0, or higher instead.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE	CVE-2005-2969

Plugin Information:

Publication date: 2005/10/12, Modification date: 2012/04/02

Ports

tcp/443

31705 - SSL Anonymous Cipher Suites Supported

Synopsis

The remote service supports the use of anonymous SSL ciphers.

Description

The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.
Note: This is considerably easier to exploit if the attacker is on the same physical network.

See Also

http://www.openssl.org/docs/apps/ciphers.html

Solution

Reconfigure the affected application if possible to avoid use of weak ciphers.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.6 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

References

BID	28482
CVE	CVE-2007-1858
XREF	OSVDB:34882

Plugin Information:

Publication date: 2008/03/28, Modification date: 2012/04/02

Ports

tcp/443

```
Here is the list of SSL anonymous ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    SSLv3
      ADH-DES-CBC3-SHA             Kx=DH           Au=None     Enc=3DES(168)            Mac=SHA1
      ADH-RC4-MD5                  Kx=DH           Au=None     Enc=RC4(128)             Mac=MD5

    TLSv1
      ADH-DES-CBC3-SHA             Kx=DH           Au=None     Enc=3DES(168)            Mac=SHA1
      ADH-AES128-SHA               Kx=DH           Au=None     Enc=AES(128)             Mac=SHA1
      ADH-AES256-SHA               Kx=DH           Au=None     Enc=AES(256)             Mac=SHA1
      ADH-CAMELLIA128-SHA          Kx=DH           Au=None     Enc=Camellia(128)        Mac=SHA1
      ADH-CAMELLIA256-SHA          Kx=DH           Au=None     Enc=Camellia(256)        Mac=SHA1
      ADH-RC4-MD5                  Kx=DH           Au=None     Enc=RC4(128)             Mac=MD5

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

62565 - TLS CRIME Vulnerability

Synopsis

The remote service has a configuration that may make it vulnerable to the CRIME attack.

Description

The remote service has one of two configurations that are known to be required for the CRIME attack:
- SSL / TLS compression is enabled.
- TLS advertises the SPDY protocol earlier than version 4.
Note that ITMS did not attempt to launch the CRIME attack against the remote service.

See Also

http://www.iacr.org/cryptodb/data/paper.php?pubkey=3091

http://www.ITMS.org/u?a1e45597 https://discussions.ITMS.org/thread/5546

http://www.ITMS.org/u?e8c92220

https://issues.apache.org/bugzilla/show_bug.cgi?id=53219

Solution

Disable compression and / or the SPDY service.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.6 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

References

BID	55704
BID	55707
CVE	CVE-2012-4929
CVE	CVE-2012-4930
XREF	OSVDB:85926
XREF	OSVDB:85927

Plugin Information:

Publication date: 2012/10/16, Modification date: 2013/01/09

Ports

tcp/443

```
The following configuration indicates that the remote service
may be vulnerable to the CRIME attack :

  - SSL / TLS compression is enabled.
```

11411 - Backup Files Disclosure

Synopsis

It is possible to retrieve file backups from the remote web server.

Description

By appending various suffixes (ie: .old, .bak, ~, etc...) to the names of various files on the remote host, it seems possible to retrieve their contents, which may result in disclosure of sensitive information.

See Also

http://projects.webappsec.org/Predictable-Resource-Location

Solution

Ensure the files do no contain any sensitive information, such as credentials to connect to a database, and delete or protect those files that should not be accessible.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin Information:

Publication date: 2003/03/17, Modification date: 2012/03/11

Ports

tcp/443

```
It is possible to read the following backup file :

  - File : /portal/logo/xxxxxx%20Logo%203.jpg~
```