Vulnerability Assessment Report for Demo Client

Author: Peter Bassill

Date: 09/08/2018

Version: 1.0

Proprietary Information

The content of this document should be considered proprietary information and should not be disclosed outside of Demo Client without their explicit permission.

Document Version Control

Classification:	Confidential
Client Name:	Demo Client
Project Ref:	DC/VA/2018
Document Title:	Vulnerability Assessment Report
Author:	Peter Bassill

Document History

Issue No	Date	Issued by	Change Description
0.1	09/08/2018	Peter Bassill	Initial version for review
0.2	09/08/2018	Peter Bassill	Technical Peer Review
0.3	09/08/2018	Cassandra Mayfield	QA Review
1.0	09/08/2018	Cassandra Mayfield	Client Release

Statement of Limitation

Hedgehog Security tested the systems defined within the scope at the requested time and is unable to comment on the security or vulnerabilities that existed prior to or after the testing was performed. All testing is time limited and it might not be possible to fully investigate every issue or find all possible security issues. Hedgehog Security are unable to comment on systems that were outside of the scope of this report or were unavailable at the time of testing or where required access was not provided.

Contents

Vulnerability Assessment Report 4
Executive Summary 4
Overall Posture 4
General Findings 4
Scope 5
Vulnerability Report 6
Vulnerability Summary Table Key 6
Vulnerability Detail Table Key 6
Summary 7
Vulnerabilities Ordered by CVSS 7
Vulnerabilities 8
Appendices 16
Appendix A: Iconography 16
Appendix B: Your Testing Team 16
Appendix C: SSL Issues 17

Vulnerability Assessment Report

Executive Summary

Demo Client sought to confirm the security of their digital infrastructure through a CREST approved vulnerability scan. The objective of this scan was to determine if there any known vulnerabilities present on the systems.

Overall Posture

Hedgehog Security conducted the vulnerability scan on 09/08/2018. The test was carried out by Peter Bassill.

General Findings

The table below shows to the most severe risks that should to be addressed along with the overall Security Rating and Risk Level for the scope.

Vulnerabilities										
Vulnerability							**CVSS**	**Exploitable**	**Risk**	
Out of date Web Server							7.8	Yes	High	
Multiple SSL Issues							7.0	Potentially	High	
Security Rating							**Risk Level**			
C	C+	B	B+	A	A+		Low	Medium	High	Critical

Security Rating Key	
A+	Excellent level of security, suitable for use in Defence and other high security environments.
A	Meets PCI-DSS standards
B+	Industry Standard and Meets Cyber Essentials Standards
B	Reasonable level of security for standard brochure sites where security isn't necessary
C+	Low level of security and needs improvements urgently.
C	Poor level of security, may be compromised imminently.

Risk Rating Key	
Low	Acceptable level of risk. Meets PCI-DSS & Cyber Essentials.
Medium	Industry Standard and Meets Cyber Essentials Standards. May meet PCI-DSS.
High	Urgent work is required to bring the risk level down to an acceptable level.
Critical	Not suitable for production environments.

Scope

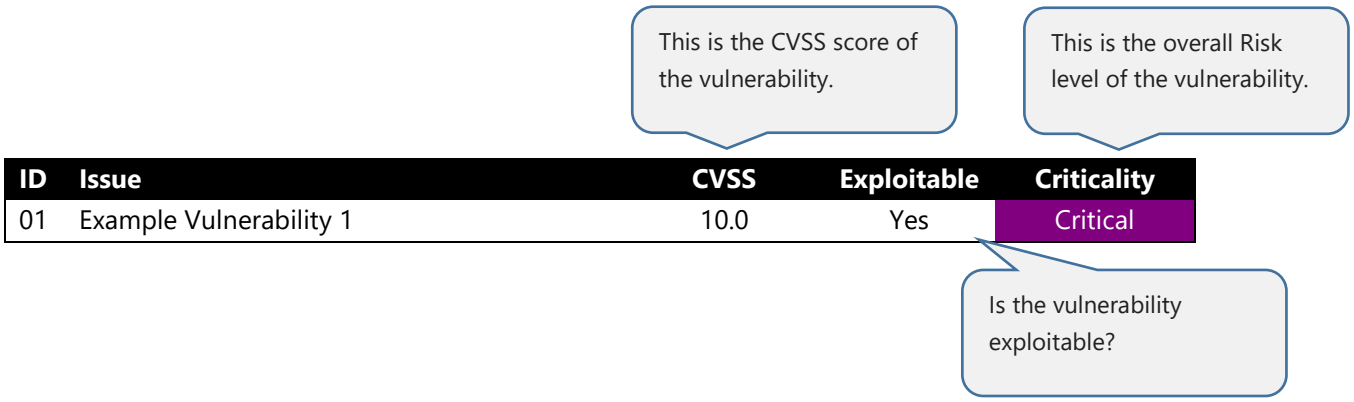
The original scope provided for a vulnerability assessment of the following:

- 192.168.1.0/24

Vulnerability Report

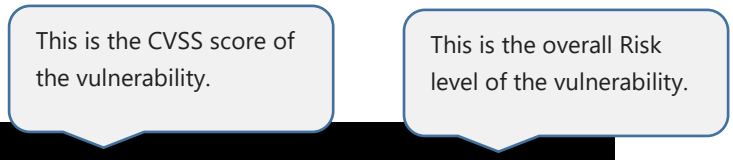
Throughout the vulnerability report we utilise two common tables that it is often valuable to explain the meanings of some of the sections.

Vulnerability Summary Table Key



ID	Issue	CVSS	Exploitable	Criticality
01	Example Vulnerability 1	10.0	Yes	Critical

Vulnerability Detail Table Key



Vulnerability Title			
Issue: **01**	Count: **4**	CVSS: **8.6**	**CRITICAL**

Summary

Vulnerabilities Ordered by CVSS

The vulnerabilities listed in the tables below are vulnerabilities which a CVSS score of 1.0 or higher. All vulnerabilities have been manually verified and all false positives have been removed.

ID	Name	CVSS	Exploitable	Severity
01	Apache 2.0.x < 2.0.65 Multiple Vulnerabilities	7.8	Yes	High
02	Unsupported Web Server Detection	7.5	No	High
03	SSL & TLS Configuration Vulnerabilities	7.0	No	High
04	HTTP TRACE / TRACK Methods Allowed	5	Yes	Medium
05	Resin Status Page Information Disclosure	5	No	Medium
06	IIS Detailed Error Information Disclosure	5	No	Medium
07	Apache HTTP Server httpOnly Cookie Information Disclosure	4.3	Yes	Medium

False Positives

The vulnerabilities listed in the table below are vulnerabilities detected by the vulnerability scanners and proved to be false positives by our penetration testing team.

Name	CVSS	Exploitable	Severity
SSL Certificate Cannot Be Trusted	6.4	No	Medium
DNS Server Spoofed Request Amplification DDoS	5	No	Medium
Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key	5	No	Medium
Web Application Potentially Vulnerable to Clickjacking	4.3	No	Medium

Vulnerabilities

Apache 2.0.x < 2.0.65 Multiple Vulnerabilities

Issue:	01	Count:	1	CVSS:	7.8	High

Description

According to its banner, the version of Apache 2.0.x running on the remote host is prior to 2.0.65. It is, therefore, affected by several vulnerabilities:

- A flaw exists in the byte-range filter, making it vulnerable to denial of service. (CVE-2011-3192)
- A flaw exists in 'mod_proxy' where it doesn't properly interact with 'RewriteRule' and 'ProxyPassMatch' in reverse proxy configurations. (CVE-2011-3368)
- A privilege escalation vulnerability exists relating to a heap-based buffer overflow in 'ap_pregsub' function in 'mod_setenvif' module via .htaccess file. (CVE-2011-3607)
- A local security bypass vulnerability exists within scoreboard shared memory that may allow the child process to cause the parent process to crash. (CVE-2012-0031)
- A flaw exists within the status 400 code when no custom ErrorDocument is specified that could disclose 'httpOnly' cookies. (CVE-2012-0053)
- A flaw exists in the 'RewriteLog' function where it fails to sanitize escape sequences written to log files, which could result in arbitrary command execution. (CVE-2013-1862)

Example Evidence

```
Version source    : Server: Apache/2.0.59 (Unix)
Installed version : 2.0.59
Fixed version     : 2.0.65
```

Affected Systems

Ports	IP(s)
80	9.demo.sec.li

Solution

Upgrade to Apache version 2.0.65 or later. Alternatively, ensure that the affected modules are not in use.

Further Information

- https://archive.apache.org/dist/httpd/CHANGES_2.0.65
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192/
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3368/
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3607/
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0031/
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0053/
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1862/

Unsupported Web Server Detection

Issue:	02	Count:	1	CVSS:	7.5	High

Description

According to its version, the remote web server is obsolete and no longer maintained by its vendor or provider. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Example Evidence

```
Product : Apache 2.0.x
Server response header: Apache/2.0.59 (Unix)
Supported versions: Apache HTTP Server 2.4.x
Additional information: http://archive.apache.org/dist/httpd/Announcement2.0.html
```

Affected Systems

Ports	IP(s)
80	9.demo.sec.li

Solution

Remove the service if it is no longer needed. Otherwise, upgrade to a newer version if possible or switch to another server.

Further Information

- http://archive.apache.org/dist/httpd/Announcement2.0.html

SSL & TLS Configuration Vulnerabilities

Issue:	03	Count:	7	CVSS:	7.0	High

Description

When reviewing the SSL & TLS configurations, we identified the following weaknesses with the certificates and configurations:

- SSL-01: SSL Version 2 and 3 enabled
- SSL-02: Expired Certificate
- SSL-03: Medium Strength Cipher Suites Supported
- SSL-04: SSL/TLS Protocol Initialization Vector Implementation
- SSL-05: SSLv3 Padding Oracle On Downgraded Legacy Encryption
- SSL-06: SSL RC4 Cipher Suites Supported
- SSL-07: SSL/TLS Diffie-Hellman Modulus <= 1024 Bits

Example Evidence

See Appendix C – SSL Issues for more information.

Affected Systems

Ports	IP(s)
443	4.demo.sec.li, 11.demo.sec.gi

Solution

Review all certificates and services and update to only use TLSv1.1 or higher with a key of at least 2048 bits.

Further Information

- https://www.schneier.com/academic/paperfiles/paper-ssl.pdf
- https://support.microsoft.com/en-us/help/187498/how-to-disable-pct-1-0-ssl-2-0-ssl-3-0-or-tls-1-0-in-internet-informat
- https://web.archive.org/web/20140909130341/http://www.linux4beginners.info/node/disable-sslv2
- https://www.openssl.org/~bodo/ssl-poodle.pdf
- https://www.pcisecuritystandards.org/pdfs/15_02_12_PCI_SSC_Bulletin_on_DSS_revisions_SSL_update.pdf
- https://www.imperialviolet.org/2014/10/14/poodle.html
- https://tools.ietf.org/html/rfc7507
- https://tools.ietf.org/html/rfc7568

HTTP TRACE / TRACK Methods Allowed

Issue:	03	Count:	2	CVSS:	5	Medium

Description

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

Example Evidence

We sent the following TRACE request:

```
---------------------------- snip ----------------------------
TRACE /HedgehogSec-2130345271.html HTTP/1.1
Connection: Close
Host: 9.demo.sec.li
---------------------------- snip ----------------------------
```

and received the following response from the remote server:

```
---------------------------- snip ----------------------------
HTTP/1.1 200 OK
Date: Sat, 04 Aug 2018 00:46:27 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips SVN/1.10.0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http
TRACE /HedgehogSec-2130345271.html HTTP/1.1
Connection: Keep-Alive
Host: 9.demo.sec.li
---------------------------- snip ----------------------------
```

Affected Systems

Ports	IP(s)
80	9.demo.sec.li
443	17.demo.sec.li

Solution

To disable these methods, add the following lines for each virtual host in your configuration file:

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2 support disabling the TRACE method natively via the 'TraceEnable' directive.

Further Information

- http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf
- http://www.apacheweek.com/issues/03-01-24
- http://download.oracle.com/sunalerts/1000718.1.html

Resin Status Page Information Disclosure

Issue:	04	Count:	1	CVSS:	5	Medium

Description

Requesting the URI '/caucho-status' or '/server-status' gives information about the currently running Resin java servlet container.

Example Evidence

The status page is available via the following URI:
`/caucho-status`

Affected Systems

Ports	IP(s)
80	5.demo.sec.li

Solution

If you don't use this feature, set the content of the '<caucho-status>' element to 'false' in the resin.conf file.

Further Information

- https://vuldb.com/?id.81831

IIS Detailed Error Information Disclosure

Issue:	05	Count:	1	CVSS:	5	Medium

Description

The remote Microsoft IIS web server is improperly configured to deliver detailed error messages. These detailed error messages may contain confidential diagnostic information, such as the file system paths to hosted content and logon information.

Example Evidence

We were able to obtain a detailed error message using the following URL:
`https://4.demo.sec.li/scripts/800624872.html`

Here is the message:

```
---------------------------- snip ----------------------------
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<title>IIS 7.5 Detailed Error - 404.0 - Not Found</title>
<h2>HTTP Error 404.0 - Not Found</h2>
<h3>The resource you are looking for has been removed, had its name changed, or is
temporarily
---------------------------- snip ----------------------------
```

Affected Systems

Ports	IP(s)
443	4.demo.sec.li

Solution

Configure the IIS server to deliver custom rather than detailed error messages.

Further Information

- https://docs.microsoft.com/en-us/iis/troubleshoot/diagnosing-http-errors/how-to-use-http-detailed-errors-in-iis
- https://blogs.msdn.microsoft.com/rakkimk/2007/05/25/iis7-how-to-enable-the-detailed-error-messages-for-the-website-while-browsed-from-for-the-client-browsers/
- http://www.iis.net/ConfigReference/system.webServer/httpErrors

Apache < 2.0.63 Multiple XSS Vulnerabilities

Issue:	06	Count:	1	CVSS:	4.3	Medium

Description

According to its banner, the version of Apache 2.0.x running on the remote host is prior to 2.0.63. It is, therefore, affected by multiple cross-site scripting vulnerabilities:

- A cross-site scripting issue involving mod_imap. (CVE-2007-5000)
- A cross-site scripting issue involving 413 error pages via a malformed HTTP method. (PR 44014 / CVE-2007-6203)
- A cross-site scripting issue in mod_status involving the refresh parameter. (CVE-2007-6388)
- A cross-site scripting issue using UTF-7 encoding in mod_proxy_ftp exists because it does not define a charset. (CVE-2008-0005)

Note that the remote web server may not actually be affected by these vulnerabilities. We did not try to determine whether the affected modules are in use or to check for the issues themselves.

Example Evidence

```
Version source    : Server: Apache/2.0.59 (Unix)
Installed version : 2.0.59
Fixed version     : 2.0.63
```

Affected Systems

Ports	IP(s)
80	9.demo.sec.li

Solution

Upgrade to Apache version 2.0.63 or later. Alternatively, ensure that he affected modules are not in use.

Further Information

- https://archive.apache.org/dist/httpd/CHANGES_2.0.63
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5000/
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6203/
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6388
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0005

Apache HTTP Server httpOnly Cookie Information Disclosure

Issue:	07	Count:	1	CVSS:	4.3	Medium

Description

The version of Apache HTTP Server running on the remote host is affected by an information disclosure vulnerability. Sending a request with HTTP headers long enough to exceed the server limit causes the web server to respond with an HTTP 400. By default, the offending HTTP header and value are displayed on the 400 error page. When used in conjunction with other attacks (e.g., cross-site scripting), this could result in the compromise of httpOnly cookies.

Example Evidence

We verified this by sending a request with a long Cookie header:

```
GET / HTTP/1.1
Host: 74.162.17.46.twi.co.uk
Accept-Charset: iso-8859-1, utf-8;q=0.9, *;q=0.1
Accept-Language: en
Connection: Close
Cookie: z9=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Which caused the Cookie header to be displayed in the default error page
(the response shown below has been truncated):
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
Size of a request header field exceeds server limit.<br />
<pre>
Cookie: z9=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...
```

Affected Systems

Ports	IP(s)
80	5.demo.sec.li

Solution

Upgrade to Apache version 2.0.65 / 2.2.22 or later.

Further Information

- http://fd.the-wildcat.de/apache_e36a9cf46c.php
- http://httpd.apache.org/security/vulnerabilities_22.html
- http://svn.apache.org/viewvc?view=revision&revision=1235454

Appendices

Appendix A: Iconography

Criticality	CVSS Score	Real World Risk	Description
CRITICAL	9.0 – 10.0	80 – 100%	The vulnerability is rated as critical and required resolution as quickly as possible.
HIGH	7.0 – 8.9	50 – 79%	The vulnerability is rated as important and requires resolution in the short term.
MEDIUM	4.0 – 6.9	20 – 49%	The vulnerability is rated as a moderate criticality and should be resolved as part of the on-going security maintenance of the affected system(s)
LOW	1.0 – 3.9	10 – 19%	The vulnerability is rated as low and should be addresses as part of routine maintenance tasks.
INFO	0 – 0.9	0 – 9%	A finding of informational value was discovered and should be addressed in order to meet leading best practice.

Appendix B: Your Testing Team

Role	Name	Qualifications
Penetration Test Team Leader:	Peter Bassill	F.BCS, C.Eng, CISSP, OSCP, CRT
Penetration Tester	-	-
QA Team Leader:	Cassandra Mayfield	

Appendix C: SSL Issues

SSL Version 2 and 3 Protocol Detection

Issue:	**SSL-01**	Count:	**1**	CVSS:	**7.0**	High

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Example Evidence

- SSLv3 is enabled and the server supports at least one cipher.

Affected Systems

Ports	**IP(s)**
443	11.demo.sec.li

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.1 (with approved cipher suites) or higher instead.

Further Information

- https://www.schneier.com/academic/paperfiles/paper-ssl.pdf
- https://support.microsoft.com/en-us/help/187498/how-to-disable-pct-1-0-ssl-2-0-ssl-3-0-or-tls-1-0-in-internet-informat
- https://web.archive.org/web/20140909130341/http://www.linux4beginners.info/node/disable-sslv2
- https://www.openssl.org/~bodo/ssl-poodle.pdf
- https://www.pcisecuritystandards.org/pdfs/15_02_12_PCI_SSC_Bulletin_on_DSS_revisions_SSL_update.pdf
- https://www.imperialviolet.org/2014/10/14/poodle.html
- https://tools.ietf.org/html/rfc7507
- https://tools.ietf.org/html/rfc7568

SSL Certificate Expiry

Issue:	SSL-02	Count:	1	CVSS:	5	Medium

Description

This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired.

Example Evidence

The SSL certificate has already expired:

```
Subject: C=GB, ST=Greater Manchester, L=Manchester, O=Demo Company, CN=*.demo.sec.li
Issuer : C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance
Server CA
Not valid before: Jul 15 00:00:00 2015 GMT
Not valid after : Aug 16 12:00:00 2016 GMT
```

Affected Systems

Ports	IP(s)
443	11.demo.sec.li

Solution

Purchase or generate a new SSL certificate to replace the existing one.

Further Information

No further information is available

SSL Medium Strength Cipher Suites Supported

Issue:	SSL-03	Count:	2	CVSS:	5	Medium

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. We regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Example Evidence

Here is the list of medium strength SSL ciphers supported by the remote server:

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

```
DES-CBC3-SHA    Kx=RSA     Au=RSA Enc=3DES-CBC(168)    Mac=SHA1
```

The fields above are:
{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

Affected Systems

Ports	IP(s)
443	11.demo.sec.li, 4.demo.sec.li

Solution

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

Further Information

- https://www.openssl.org/blog/blog/2016/08/24/sweet32/

SSL/TLS Protocol Initialization Vector Implementation

Issue:	**SSL-04**	Count:	**3**	CVSS:	**4.3**	Medium

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 plugin 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 be, depending on whether or not a countermeasure has been enabled.

Example Evidence

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

Affected Systems

Ports	**IP(s)**
443	11.demo.sec.li, 17.demo.sec.li, 4.demo.sec.li

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.

Further Information

- http://www.openssl.org/~bodo/tls-cbc.txt
- https://www.imperialviolet.org/2011/09/23/chromeandbeast.html
- http://vnhacker.blogspot.com/2011/09/beast.html
- https://technet.microsoft.com/library/security/ms12-006
- https://support.microsoft.com/en-us/kb/2643584
- http://blogs.msdn.com/b/kaushal/archive/2012/01/21/fixing-the-beast.aspx

SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability

Issue:	SSL-05	Count:	1	CVSS:	4.3	Medium

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

Example Evidence

We determined that the remote server supports SSLv3 with at least one CBC cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the Fallback SCSV mechanism is not supported, allowing connections to be "rolled back" to SSLv3.

Affected Systems

Ports	IP(s)
443	11.demo.sec.li

Solution

Disable SSLv3.
Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Further Information

- https://www.imperialviolet.org/2014/10/14/poodle.html
- https://www.openssl.org/~bodo/ssl-poodle.pdf
- https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

SSL RC4 Cipher Suites Supported

Issue:	**SSL-06**	Count:	**2**	CVSS:	**2.6**	Low

Description

The remote host supports the use of RC4 in one or more cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

Example Evidence

List of RC4 cipher suites supported by the remote server:

High Strength Ciphers (>= 112-bit key)

```
RC4-SHA    Kx=RSA     Au=RSA  Enc=RC4(128)    Mac=SHA1
```

The fields above are:
{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

Affected Systems

Ports	**IP(s)**
443	11.demo.sec.li, 4.demo.sec.li

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Further Information

- https://blog.cryptographyengineering.com/2013/03/12/attack-of-week-rc4-is-kind-of-broken-in/
- http://cr.yp.to/talks/2013.03.12/slides.pdf
- http://www.isg.rhul.ac.uk/tls/
- http://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

SSL/TLS Diffie-Hellman Modulus <= 1024 Bits

Issue:	**SSL-07**	Count:	**1**	CVSS:	**2.6**	Low

Description

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.

Example Evidence

Vulnerable connection combinations:

```
SSL/TLS version : TLSv1.0
Cipher suite: TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA
Diffie-Hellman MODP size (bits): 1024
Warning - This is a known static Oakley Group2 modulus. This may make the remote host
more vulnerable to the Logjam attack.
Logjam attack difficulty: Hard (would require nation-state resources)

SSL/TLS version : TLSv1.0
Cipher suite: TLS1_CK_DHE_RSA_WITH_AES_128_CBC_SHA
Diffie-Hellman MODP size (bits): 1024
Warning - This is a known static Oakley Group2 modulus. This may make the remote host
more vulnerable to the Logjam attack.
Logjam attack difficulty: Hard (would require nation-state resources)
```

Affected Systems

Ports	**IP(s)**
443	11.demo.sec.li

Solution

Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.

Further Information

- http://weakdh.org/