Scan Results

Datum

Report Summary	
User Name:	
Login Name:	
Company:	
User Role:	
Address:	
City:	
Zip:	
Country:	
Created:	
Client:	
Launch Date:	
Active Hosts:	
Total Hosts:	25
Type:	Scheduled
Status:	Finished
Reference:	
External Scanners:	154.59.121.134 (Scanner 10.3.48-1, Vulnerability Signatures 2.4.402-2)
Duration:	01:05:00
Title:	PST | External IP
Asset Groups:	PST | External IP
IPs:	
Excluded IPs:	-
Options Profile:	Initial Options

Summary of Vulnerabilities

Vulnerabilities Total	541

Security Risk (Avg)	1.6

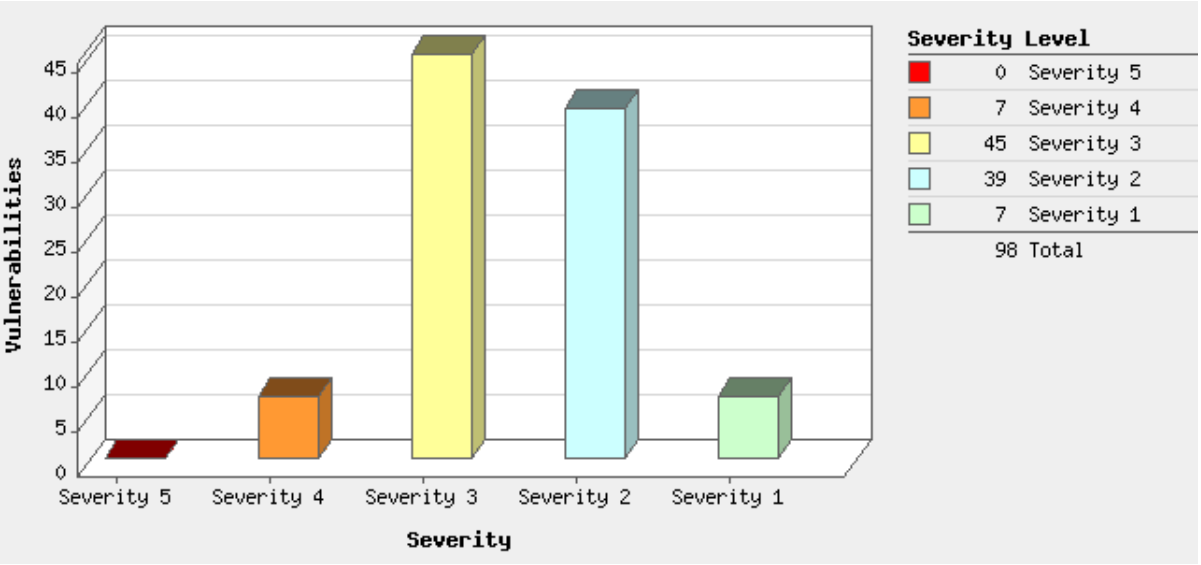
by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	0	1	0	1
4	7	0	0	7
3	45	7	9	61
2	39	1	48	88
1	7	0	377	384
Total	98	9	434	541

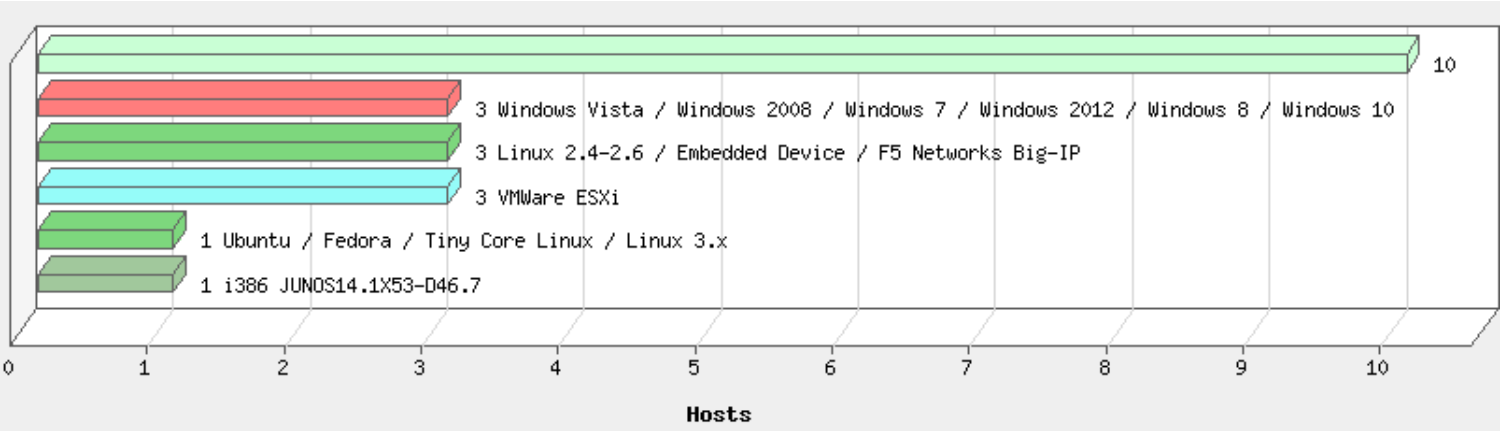
5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
General remote services	72	1	120	193
Information gathering	1	0	148	149
TCP/IP	6	0	68	74
Web server	3	0	48	51
CGI	9	1	15	25
Total	91	2	399	492

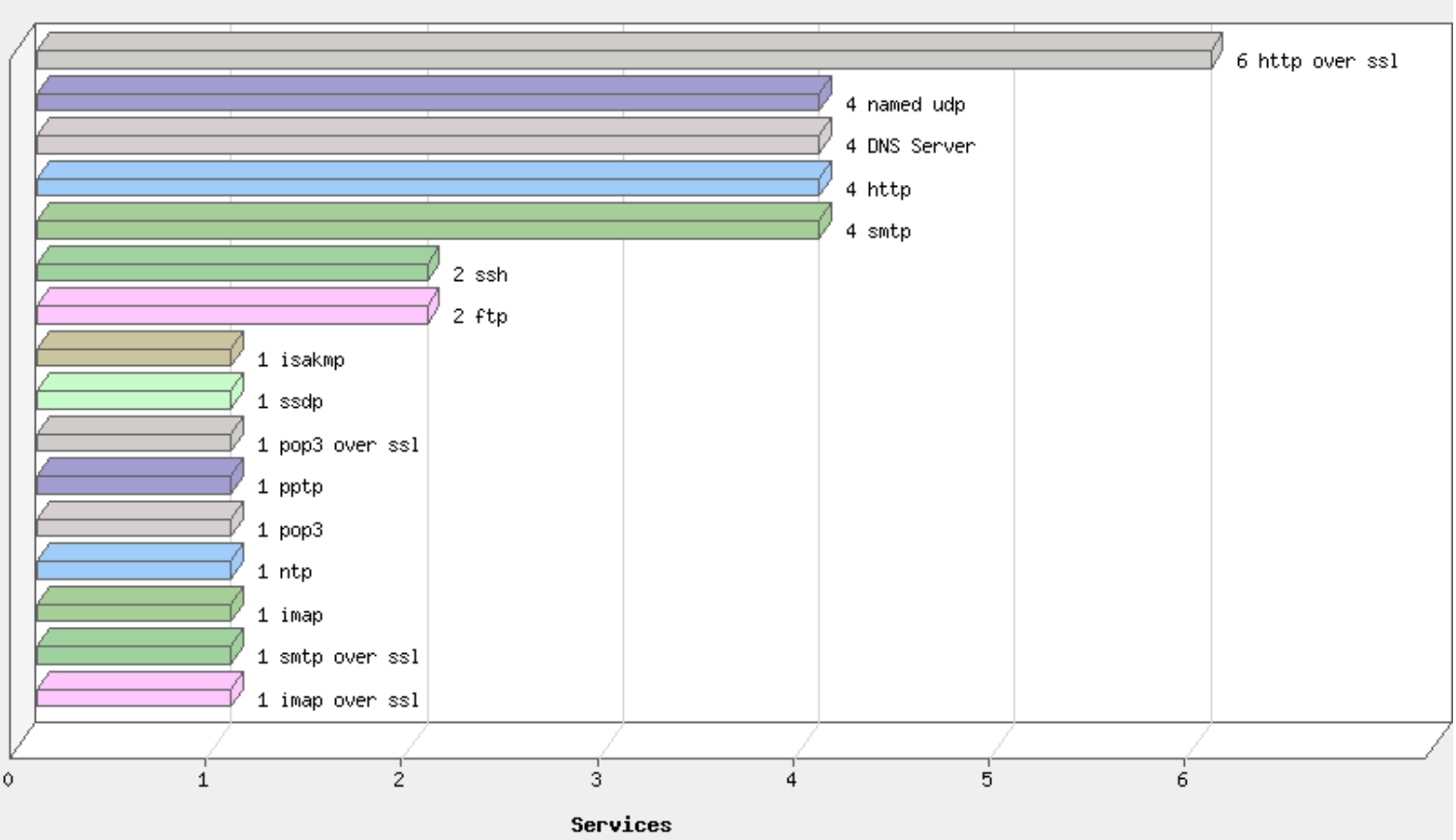
Vulnerabilities by Severity



Operating Systems Detected



Services Detected



Detailed Results

Hostname : IP ADDRESS — Ubuntu / Fedora / Tiny Core Linux / Linux 3.x

Vulnerabilities (56)

4 SSL Server Allows Anonymous Authentication Vulnerability — port 465/tcp over SSL

QID:	38142
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/31/2018
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The Secure Socket Layer (SSL) protocol allows for secure communication between a client and a server. The client usually authenticates the server using an algorithm like RSA or DSS. Some SSL ciphers allow SSL communication without authentication. Most common Web browsers like Microsoft Internet Explorer, Netscape and Mozilla do not use anonymous authentication ciphers by default.
A vulnerability exists in SSL communications when clients are allowed to connect
using no authentication algorithm. SSL client-server communication may use several different types of
authentication: RSA, Diffie-Hellman, DSS or none. When 'none' is used, the
communications are vulnerable to a man-in-the-middle attack."

IMPACT:

An attacker can exploit this vulnerability to impersonate your server to clients.

SOLUTION:
It is recommended that you follow SSL best security practices:
SSL and TLS Deployment Best Practices (https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices)
http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-1/ssl.html (http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-1/ssl.html)
http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite (http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite)
Example: Disable support for anonymous authentication.
1) How to disable for Apache:
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 include the following line in the configuration file (httpsd.conf):
SSLRequireCipher ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
2) IIS:
For IIS please see: How to disable PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services (http://support.microsoft.com/kb/187498/en-us), How to Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll (http://support.microsoft.com/kb/245030/en-us), How to Determine the Cipher Suite for the Server and Client (http://support.microsoft.com/kb/299520/en-us).
3) Wu-FTP:
For Wu-FTP which supports TLS, the ciphers parameter in TLS configuration file should be set to -ALL +SSLv3 +TLSv1 For more details please consult the docs/HOWTO/ssl_and_tls_ftpd.HOWTO file provided by wu-ftpd distribution.
4) Lighttpd:
For lighttpd: Locate the lighttpd config file and modify the following ssl.ciper-list line to include !aNULL. A restart of the lightttpd application is necessary.
Example: ssl.cipher-list = "TLSv1+HIGH !SSLv2 RC4+MEDIUM !aNULL !eNULL !3DES @STRENGTH"

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
TLSv1 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH
TLSv1.1 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH
TLSv1.2 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH

4 SSL Server Allows Anonymous Authentication Vulnerability port 110/tcp over SSL

QID:	38142
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/31/2018
User Modified:	-
Edited:	No

PCI Vuln: Yes

THREAT:

The Secure Socket Layer (SSL) protocol allows for secure communication between a client and a server. The client usually authenticates the server using an algorithm like RSA or DSS. Some SSL ciphers allow SSL communication without authentication. Most common Web browsers like Microsoft Internet Explorer, Netscape and Mozilla do not use anonymous authentication ciphers by default.
A vulnerability exists in SSL communications when clients are allowed to connect
using no authentication algorithm. SSL client-server communication may use several different types of
authentication: RSA, Diffie-Hellman, DSS or none. When 'none' is used, the
communications are vulnerable to a man-in-the-middle attack."

IMPACT:

An attacker can exploit this vulnerability to impersonate your server to clients.

SOLUTION:

It is recommended that you follow SSL best security practices:
SSL and TLS Deployment Best Practices (https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices)
http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-1/ssl.html (http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-1/ssl.html)
http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite (http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite)
Example: Disable support for anonymous authentication.
1) How to disable for Apache:
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 include the following line in the configuration file (httpsd.conf):
SSLRequireCipher ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
2) IIS:
For IIS please see: How to disable PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services (http://support.microsoft.com/kb/187498/en-us), How to Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll (http://support.microsoft.com/kb/245030/en-us), How to Determine the Cipher Suite for the Server and Client (http://support.microsoft.com/kb/299520/en-us).
3) Wu-FTP:
For Wu-FTP which supports TLS, the ciphers parameter in TLS configuration file should be set to -ALL +SSLv3 +TLSv1 For more details please consult the docs/HOWTO/ssl_and_tls_ftpd.HOWTO file provided by wu-ftpd distribution.
4) Lighttpd:
For lighttpd: Locate the lighttpd config file and modify the following ssl.ciper-list line to include !aNULL. A restart of the lightttpd application is necessary.
Example: ssl.cipher-list = "TLSv1+HIGH !SSLv2 RC4+MEDIUM !aNULL !eNULL !3DES @STRENGTH"

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
TLSv1 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH
TLSv1.1 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH
TLSv1.2 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM

AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH

4 SSL Server Allows Anonymous Authentication Vulnerability port 143/tcp over SSL

QID:	38142
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/31/2018
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The Secure Socket Layer (SSL) protocol allows for secure communication between a client and a server. The client usually authenticates the server using an algorithm like RSA or DSS. Some SSL ciphers allow SSL communication without authentication. Most common Web browsers like Microsoft Internet Explorer, Netscape and Mozilla do not use anonymous authentication ciphers by default.
A vulnerability exists in SSL communications when clients are allowed to connect
using no authentication algorithm. SSL client-server communication may use several different types of
authentication: RSA, Diffie-Hellman, DSS or none. When 'none' is used, the
communications are vulnerable to a man-in-the-middle attack."

IMPACT:

An attacker can exploit this vulnerability to impersonate your server to clients.

SOLUTION:

It is recommended that you follow SSL best security practices:
SSL and TLS Deployment Best Practices (https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices)
http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-1/ssl.html (http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-1/ssl.html)
http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite (http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite)
Example: Disable support for anonymous authentication.
1) How to disable for Apache:
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 include the following line in the configuration file (httpsd.conf):
SSLRequireCipher ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
2) IIS:
For IIS please see: How to disable PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services (http://support.microsoft.com/kb/187498/en-us), How to Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll (http://support.microsoft.com/kb/245030/en-us), How to Determine the Cipher Suite for the Server and Client (http://support.microsoft.com/kb/299520/en-us).
3) Wu-FTP:
For Wu-FTP which supports TLS, the ciphers parameter in TLS configuration file should be set to -ALL +SSLv3 +TLSv1 For more details please consult the docs/HOWTO/ssl_and_tls_ftpd.HOWTO file provided by wu-ftpd distribution.
4) Lighttpd:
For lighttpd: Locate the lighttpd config file and modify the following ssl.ciper-list line to include !aNULL. A restart of the lightttpd application is necessary.
Example: ssl.cipher-list = "TLSv1+HIGH !SSLv2 RC4+MEDIUM !aNULL !eNULL !3DES @STRENGTH"

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
TLSv1 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM

AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH
TLSv1.1 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH
TLSv1.2 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH

4 SSL Server Allows Anonymous Authentication Vulnerability

port 25/tcp over SSL

QID:	38142
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/31/2018
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The Secure Socket Layer (SSL) protocol allows for secure communication between a client and a server. The client usually authenticates the server using an algorithm like RSA or DSS. Some SSL ciphers allow SSL communication without authentication. Most common Web browsers like Microsoft Internet Explorer, Netscape and Mozilla do not use anonymous authentication ciphers by default.
A vulnerability exists in SSL communications when clients are allowed to connect
using no authentication algorithm. SSL client-server communication may use several different types of
authentication: RSA, Diffie-Hellman, DSS or none. When 'none' is used, the
communications are vulnerable to a man-in-the-middle attack."

IMPACT:

An attacker can exploit this vulnerability to impersonate your server to clients.

SOLUTION:

It is recommended that you follow SSL best security practices:
SSL and TLS Deployment Best Practices (https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices)
http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-1/ssl.html (http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-1/ssl.html)
http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite (http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite)
Example: Disable support for anonymous authentication.
1) How to disable for Apache:
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 include the following line in the configuration file (httpsd.conf):
SSLRequireCipher ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
2) IIS:
For IIS please see: How to disable PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services (http://support.microsoft.com/kb/187498/en-us), How to Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll (http://support.microsoft.com/kb/245030/en-us), How to Determine the Cipher Suite for the Server and Client (http://support.microsoft.com/kb/299520/en-us).
3) Wu-FTP:
For Wu-FTP which supports TLS, the ciphers parameter in TLS configuration file should be set to -ALL +SSLv3 +TLSv1 For more details please consult the docs/HOWTO/ssl_and_tls_ftpd.HOWTO file provided by wu-ftpd distribution.
4) Lighttpd:
For lighttpd: Locate the lighttpd config file and modify the following ssl.ciper-list line to include !aNULL. A restart of the lightttpd application is necessary.
Example: ssl.cipher-list = "TLSv1+HIGH !SSLv2 RC4+MEDIUM !aNULL !eNULL !3DES @STRENGTH"

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
TLSv1 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH
TLSv1.1 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH
TLSv1.2 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH

4 SSL Server Allows Anonymous Authentication Vulnerability

port 587/tcp over SSL

QID:	38142
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/31/2018
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
The Secure Socket Layer (SSL) protocol allows for secure communication between a client and a server. The client usually authenticates the server using an algorithm like RSA or DSS. Some SSL ciphers allow SSL communication without authentication. Most common Web browsers like Microsoft Internet Explorer, Netscape and Mozilla do not use anonymous authentication ciphers by default.
A vulnerability exists in SSL communications when clients are allowed to connect
using no authentication algorithm. SSL client-server communication may use several different types of
authentication: RSA, Diffie-Hellman, DSS or none. When 'none' is used, the
communications are vulnerable to a man-in-the-middle attack."

IMPACT:
An attacker can exploit this vulnerability to impersonate your server to clients.

SOLUTION:
It is recommended that you follow SSL best security practices:
SSL and TLS Deployment Best Practices (https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices)
http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-1/ssl.html (http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-1/ssl.html)
http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite (http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite)
Example: Disable support for anonymous authentication.
1) How to disable for Apache:
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 include the following line in the configuration file (httpsd.conf):
SSLRequireCipher ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
2) IIS:
For IIS please see: How to disable PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services (http://support.microsoft.com/kb/187498/en-us), How to Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll (http://support.microsoft.com/kb/245030/en-us), How to Determine the Cipher Suite for the Server and Client (http://support.microsoft.com/kb/299520/en-us).
3) Wu-FTP:
For Wu-FTP which supports TLS, the ciphers parameter in TLS configuration file should be set to -ALL +SSLv3 +TLSv1 For more details please consult the docs/HOWTO/ssl_and_tls_ftpd.HOWTO file provided by wu-ftpd distribution.
4) Lighttpd:
For lighttpd: Locate the lighttpd config file and modify the following ssl.ciper-list line to include !aNULL. A restart of the lightttpd application is necessary.
Example: ssl.cipher-list = "TLSv1+HIGH !SSLv2 RC4+MEDIUM !aNULL !eNULL !3DES @STRENGTH"

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
TLSv1 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH
TLSv1.1 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH
TLSv1.2 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH

4 SSL Server Allows Anonymous Authentication Vulnerability

port 993/tcp over SSL

QID:	38142
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/31/2018
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
The Secure Socket Layer (SSL) protocol allows for secure communication between a client and a server. The client usually authenticates the server using an algorithm like RSA or DSS. Some SSL ciphers allow SSL communication without authentication. Most common Web browsers like Microsoft Internet Explorer, Netscape and Mozilla do not use anonymous authentication ciphers by default.
A vulnerability exists in SSL communications when clients are allowed to connect

using no authentication algorithm. SSL client-server communication may use several different types of authentication: RSA, Diffie-Hellman, DSS or none. When 'none' is used, the communications are vulnerable to a man-in-the-middle attack."

IMPACT:
An attacker can exploit this vulnerability to impersonate your server to clients.

SOLUTION:
It is recommended that you follow SSL best security practices:
SSL and TLS Deployment Best Practices (https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices)
http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-1/ssl.html (http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-1/ssl.html)
http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite (http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite)
Example: Disable support for anonymous authentication.
1) How to disable for Apache:
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 include the following line in the configuration file (httpsd.conf):
SSLRequireCipher ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
2) IIS:
For IIS please see: How to disable PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services (http://support.microsoft.com/kb/187498/en-us), How to Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll (http://support.microsoft.com/kb/245030/en-us), How to Determine the Cipher Suite for the Server and Client (http://support.microsoft.com/kb/299520/en-us).
3) Wu-FTP:
For Wu-FTP which supports TLS, the ciphers parameter in TLS configuration file should be set to -ALL +SSLv3 +TLSv1 For more details please consult the docs/HOWTO/ssl_and_tls_ftpd.HOWTO file provided by wu-ftpd distribution.
4) Lighttpd:
For lighttpd: Locate the lighttpd config file and modify the following ssl.ciper-list line to include !aNULL. A restart of the lightttpd application is necessary.
Example: ssl.cipher-list = "TLSv1+HIGH !SSLv2 RC4+MEDIUM !aNULL !eNULL !3DES @STRENGTH"

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
TLSv1 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH
TLSv1.1 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH
TLSv1.2 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH

4 SSL Server Allows Anonymous Authentication Vulnerability port 995/tcp over SSL

QID: 38142
Category: General remote services
CVE ID: -

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/31/2018
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The Secure Socket Layer (SSL) protocol allows for secure communication between a client and a server. The client usually authenticates the server using an algorithm like RSA or DSS. Some SSL ciphers allow SSL communication without authentication. Most common Web browsers like Microsoft Internet Explorer, Netscape and Mozilla do not use anonymous authentication ciphers by default.
A vulnerability exists in SSL communications when clients are allowed to connect
using no authentication algorithm. SSL client-server communication may use several different types of
authentication: RSA, Diffie-Hellman, DSS or none. When 'none' is used, the
communications are vulnerable to a man-in-the-middle attack."

IMPACT:

An attacker can exploit this vulnerability to impersonate your server to clients.

SOLUTION:

It is recommended that you follow SSL best security practices:
SSL and TLS Deployment Best Practices (https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices)
http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-1/ssl.html (http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-1/ssl.html)
http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite (http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite)
Example: Disable support for anonymous authentication.
1) How to disable for Apache:
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 include the following line in the configuration file (httpsd.conf):
SSLRequireCipher ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
2) IIS:
For IIS please see: How to disable PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services (http://support.microsoft.com/kb/187498/en-us), How to Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll (http://support.microsoft.com/kb/245030/en-us), How to Determine the Cipher Suite for the Server and Client (http://support.microsoft.com/kb/299520/en-us).
3) Wu-FTP:
For Wu-FTP which supports TLS, the ciphers parameter in TLS configuration file should be set to -ALL +SSLv3 +TLSv1 For more details please consult the docs/HOWTO/ssl_and_tls_ftpd.HOWTO file provided by wu-ftpd distribution.
4) Lighttpd:
For lighttpd: Locate the lighttpd config file and modify the following ssl.ciper-list line to include !aNULL. A restart of the lightttpd application is necessary.
Example: ssl.cipher-list = "TLSv1+HIGH !SSLv2 RC4+MEDIUM !aNULL !eNULL !3DES @STRENGTH"

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
TLSv1 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH
TLSv1.1 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM

AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH
TLSv1.2 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH

3 SSL/TLS Server supports TLSv1.0 port 443/tcp over SSL

QID:	38628
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/20/2018
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs.
For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.
RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack.
TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security.
A POODLE-type (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) attack could also be launched directly at TLS without negotiating a downgrade.
This QID is a PCI FAIL in accordance with the PCI standards.

Further details can be found under: PCI: Use of SSL Early TLS and ASV Scans (https://www.pcisecuritystandards.org/documents/Use-of-SSL-Early-TLS-and-ASV-Scans.pdf)

IMPACT:

An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications.
For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages.
A POODLE-type (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) attack could also be launched directly at TLS without negotiating a downgrade.

SOLUTION:

Disable the use of TLSv1.0 protocol in favor of a cryptographically stronger protocol such as TLSv1.2.
The following openssl commands can be used
to do a manual test:
openssl s_client -connect ip:port -tls1

If the test is successful, then the target support TLSv1

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.0 is supported

3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) port 443/tcp over SSL

QID:	38657
Category:	General remote services
CVE ID:	CVE-2016-2183
Vendor Reference:	-
Bugtraq ID:	92630, 95568
Service Modified:	05/30/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Legacy block ciphers having block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode.
All versions of SSL/TLS
protocol support cipher suites which use DES, 3DES, IDEA or RC2 as the symmetric encryption cipher are affected.

IMPACT:
Remote attackers can obtain cleartext data via a birthday attack against a long-duration encrypted session.

SOLUTION:
Disable and stop using DES, 3DES, IDEA or RC2 ciphers.

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
TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM

3 PhpMyAdmin Multiple Vulnerabilities (Hostnames) port 80/tcp

QID:	13174
Category:	CGI
CVE ID:	CVE-2018-12581, CVE-2018-12613
Vendor Reference:	-
Bugtraq ID:	104222, 104178, 104530, 104532
Service Modified:	08/18/2018
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PhpMyAdmin is a free software tool written in PHP and intended to handle the administration of MySQL over the Internet.
Multiple vulnerabilities were reported in PhpMyAdmin
CVE-2018-12581:A Cross-Site Scripting vulnerability has been found where an attacker can use a crafted database name to trigger an XSS attack when that database is referenced from the Designer feature.
CVE-2018-12613: An issue was discovered in phpMyAdmin, in which an attacker can include (view and potentially execute) files on the server. The vulnerability comes from a portion of code where pages are redirected and loaded within phpMyAdmin, and an improper test for whitelisted pages. An attacker must be authenticated, except in the "$cfg['AllowArbitraryServer'] = true" case (where an attacker can specify any host he/she is already in control of, and execute arbitrary code on phpMyAdmin) and the "$cfg['ServerDefault'] = 0" case (which bypasses the login requirement and runs the vulnerable code without any authentication).
Affected Versions:
phpMyAdmin versions prior to 4.8.2
QID Detection Logic (Unauthenticated):
This checks for vulnerable versions of phpMyadmin in Http header

IMPACT:

Successful exploitation can result in file inclusion ,remote code execution and cross-site-scripting attack.

SOLUTION:

Users are advised to upgrade to phpMyAdmin 4.8.2 or newer from phpMyAdmin (http://phpmyadmin.net/home_page/downloads.php).
For more information check PMASA-2018-3 (https://www.phpmyadmin.net/security/PMASA-2018-3/) and PMASA-2018-4 (https://www.phpmyadmin.net/security/PMASA-2018-4/).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
PMASA-2018-3: PhpMyAdmin (https://www.phpmyadmin.net/security/PMASA-2018-3/)
PMASA-2018-4: PhpMyAdmin (https://www.phpmyadmin.net/security/PMASA-2018-4/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Metasploit

Reference:	CVE-2018-12613
Description:	phpMyAdmin Authenticated Remote Code Execution - Metasploit Ref : /modules/exploit/multi/http/phpmyadmin_lfi_rce
Link:	https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/http/phpmyadmin_lfi_rce.rb

The Exploit-DB

Reference:	CVE-2018-12613
Description:	phpMyAdmin - (Authenticated) Remote Code Execution (Metasploit) - The Exploit-DB Ref : 45020
Link:	http://www.exploit-db.com/exploits/45020

Reference:	CVE-2018-12613
Description:	phpMyAdmin 4.8.1 - (Authenticated) Local File Inclusion (1) - The Exploit-DB Ref : 44924
Link:	http://www.exploit-db.com/exploits/44924

Reference:	CVE-2018-12613
Description:	phpMyAdmin 4.8.1 - (Authenticated) Local File Inclusion (2) - The Exploit-DB Ref : 44928
Link:	http://www.exploit-db.com/exploits/44928

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable PhpMyAdmin Detected on port: 80
"phpMyAdmin 4.8.1 documentation"

3 PhpMyAdmin Multiple Vulnerabilities (Hostnames) port 443/tcp

QID:	13174
Category:	CGI
CVE ID:	CVE-2018-12581, CVE-2018-12613
Vendor Reference:	PMASA-2018-3, PMASA-2018-4
Bugtraq ID:	104222, 104178, 104530, 104532
Service Modified:	08/18/2018
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

PhpMyAdmin is a free software tool written in PHP and intended to handle the administration of MySQL over the Internet.
Multiple vulnerabilities were reported in PhpMyAdmin
CVE-2018-12581:A Cross-Site Scripting vulnerability has been found where an attacker can use a crafted database name to trigger an XSS attack when that database is referenced from the Designer feature.
CVE-2018-12613: An issue was discovered in phpMyAdmin, in which an attacker can include (view and potentially execute) files on the server. The vulnerability comes from a portion of code where pages are redirected and loaded within phpMyAdmin, and an improper test for whitelisted pages. An attacker must be authenticated, except in the "$cfg['AllowArbitraryServer'] = true" case (where an attacker can specify any host he/she is already in control of, and execute arbitrary code on phpMyAdmin) and the "$cfg['ServerDefault'] = 0" case (which bypasses the login requirement and runs the vulnerable code without any authentication).
Affected Versions:
phpMyAdmin versions prior to 4.8.2
QID Detection Logic (Unauthenticated):
This checks for vulnerable versions of phpMyadmin in Http header

IMPACT:

Successful exploitation can result in file inclusion ,remote code execution and cross-site-scripting attack.

SOLUTION:

Users are advised to upgrade to phpMyAdmin 4.8.2 or newer from phpMyAdmin (http://phpmyadmin.net/home_page/downloads.php).
For more information check PMASA-2018-3 (https://www.phpmyadmin.net/security/PMASA-2018-3/) and PMASA-2018-4 (https://www.phpmyadmin.net/security/PMASA-2018-4/).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
PMASA-2018-3: PhpMyAdmin (https://www.phpmyadmin.net/security/PMASA-2018-3/)
PMASA-2018-4: PhpMyAdmin (https://www.phpmyadmin.net/security/PMASA-2018-4/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Metasploit

Reference:	CVE-2018-12613
Description:	phpMyAdmin Authenticated Remote Code Execution - Metasploit Ref : /modules/exploit/multi/http/phpmyadmin_lfi_rce
Link:	https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/http/phpmyadmin_lfi_rce.rb

The Exploit-DB

Reference:	CVE-2018-12613
Description:	phpMyAdmin - (Authenticated) Remote Code Execution (Metasploit) - The Exploit-DB Ref : 45020
Link:	http://www.exploit-db.com/exploits/45020

Reference:	CVE-2018-12613
Description:	phpMyAdmin 4.8.1 - (Authenticated) Local File Inclusion (1) - The Exploit-DB Ref : 44924
Link:	http://www.exploit-db.com/exploits/44924

Reference:	CVE-2018-12613
Description:	phpMyAdmin 4.8.1 - (Authenticated) Local File Inclusion (2) - The Exploit-DB Ref : 44928
Link:	http://www.exploit-db.com/exploits/44928

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable PhpMyAdmin Detected on port: 443
"phpMyAdmin 4.8.1 documentation"

3 Apple MacOS X .DS_Store Directory Listing Disclosure Vulnerability — port 443/tcp

QID:	86251
Category:	Web server
CVE ID:	CVE-2001-1446
Vendor Reference:	-
Bugtraq ID:	3324, 3325
Service Modified:	02/14/2018

User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

A '.DS_Store' file found on the target.
The .DS_Store file is created by the Macintosh OS X Finder.
.DS_Store files contain some vital folder information that can be exploited to obtain sensitive information about system configurations, installed applications, Apple Spotlight comments, etc.
For example: A remote attacker can read this directory content information by submitting a URL to the vulnerable host's Web service in the following format: http://www.example.com/target_directory/.DS_store.
This vulnerability can be present on any web-servers which host content that is copied from a developer's MacOS X workstation.
QID Detection Logic (remote):
The detection detected a .DS_Store file on the target by asking for the .DS_Store file.

IMPACT:

This vulnerability could allow an attacker to obtain sensitive information about your system, including system configuration settings, installed applications Apple Spotlight comments, etc.
If this vulnerability is properly exploited, the information gathered could allow an attacker to further compromise the security of the host.

SOLUTION:

Apple Macintosh users should configure their workstation to disable the creation of .DS_Store files on network shares.
How to prevent .DS_Store file creation over network connections (https://support.apple.com/en-us/HT1629)
Use Unix file permissions or Apache run-time configuration directives to limit access to the hidden index data file.
Workaround:
Use Unix file permissions or Apache run-time configuration directives to limit access to the hidden index data file.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET /.DS_Store HTTP/1.0
Host: name

3 Apple Macintosh OS X Client Apache Directory Contents Disclosure Vulnerability port 443/tcp

QID:	86252
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	3316
Service Modified:	02/14/2018
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

A vulnerability exists when Apache Web Server is used with the MacOS X Client.
Due to a flaw in Mac OS file permissions, an issue exists which could disclose the contents of a particular Web directory to an unauthorized user.
Requesting a URL with the relative path of a '.DS_Store' file, will reveal the contents of the requested directory.
The .DS_Store file is created by the Macintosh OS X Finder.
.DS_Store files contain some vital folder information that can be exploited to obtain sensitive information about system configurations, installed applications, Apple Spotlight comments, etc.
This vulnerability can be present on any web-servers which host content that is copied from a developer's MacOS X workstation.

QID Detection Logic (remote):
The detection detected a .DS_Store file on the target by asking for the .DS_Store file.

IMPACT:
If exploited, this vulnerability could allow the contents of a particular Web directory to be disclosed to an unauthorized user.
This vulnerability could also be used in conjunction with a previously discovered issue (Qualys ID 86251), which causes files to be arbitrarily disclosed through mixed case file requests.

SOLUTION:
Apple Macintosh users should configure their workstation to disable the creation of .DS_Store files on network shares.
How to prevent .DS_Store file creation over network connections (https://support.apple.com/en-us/HT1629)
Use Unix file permissions or Apache run-time configuration directives to limit access to the hidden index data file.
Disallow remote access to .DS_store files.
Workaround:
Use Unix file permissions or Apache run-time configuration directives to limit access to the hidden index data file.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:
No results available

3 SSL/TLS use of weak RC4 cipher — port 465/tcp over SSL

QID:	38601
Category:	General remote services
CVE ID:	CVE-2013-2566, CVE-2015-2808
Vendor Reference:	-
Bugtraq ID:	91787, 58796, 73684
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS) protocols provide integrity, confidentiality and authenticity services to other protocols that lack these features.
SSL/TLS protocols use ciphers such as AES,DES, 3DES and RC4 to encrypt the content of the higher layer protocols and thus provide the confidentiality service. Normally the output of an encryption process is a sequence of random looking bytes. It was known that RC4 output has some bias in the output. Recently a group of researchers has discovered that the there is a stronger bias in RC4, which make statistical analysis of ciphertext more practical.
The described attack is to inject a malicious javascript into the victim's browser that would ensure that there are multiple connections being established with a target website and the same HTTP cookie is sent multiple times to the website in encrypted form. This provides the attacker a large set of ciphertext samples, that can be used for statistical analysis.
NOTE: On 3/12/15 NVD changed the CVSS v2 access complicity from high to medium. As a result Qualys revised the CVSS score to 4.3 immediately. On 5/4/15 Qualys is also revising the severity to level 3.

IMPACT:
If this attack is carried out and an HTTP cookie is recovered, then the attacker can use the cookie to impersonate the user whose cookie was recovered.
This attack is not very practical as it requires the attacker to have access to millions of samples of ciphertext, but there are certain assumptions that an attacker can make to improve the chances of recovering the cleartext from cihpertext. For examples HTTP cookies are either base64 encoded or hex digits. This information can help the attacker in their efforts to recover the cookie.

SOLUTION:
RC4 should not be used where possible. One reason that RC4 was still being used was BEAST and Lucky13 attacks against CBC mode ciphers in SSL and

TLS. However, TLSv 1.2 or later address these issues.

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
TLSv1 WITH RC4 CIPHERS IS SUPPORTED					
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED					
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED					
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM

 3 SSL/TLS Server supports TLSv1.0 port 465/tcp over SSL

QID:	38628
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/20/2018
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs.
For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.
RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack.
TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security.
A POODLE-type (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) attack could also be launched directly at TLS without negotiating a downgrade.
This QID is a PCI FAIL in accordance with the PCI standards.

Further details can be found under: PCI: Use of SSL Early TLS and ASV Scans (https://www.pcisecuritystandards.org/documents/Use-of-SSL-Early-TLS-and-ASV-Scans.pdf)

IMPACT:
An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications.
For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages.

A POODLE-type (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) attack could also be launched directly at TLS without negotiating a downgrade.

SOLUTION:
Disable the use of TLSv1.0 protocol in favor of a cryptographically stronger protocol such as TLSv1.2.
The following openssl commands can be used
to do a manual test:
openssl s_client -connect ip:port -tls1

If the test is successful, then the target support TLSv1

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:
TLSv1.0 is supported

3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) port 465/tcp over SSL

QID:	38657
Category:	General remote services
CVE ID:	CVE-2016-2183
Vendor Reference:	-
Bugtraq ID:	92630, 95568
Service Modified:	05/30/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Legacy block ciphers having block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode.
All versions of SSL/TLS
protocol support cipher suites which use DES, 3DES, IDEA or RC2 as the symmetric encryption cipher are affected.

IMPACT:
Remote attackers can obtain cleartext data via a birthday attack against a long-duration encrypted session.

SOLUTION:
Disable and stop using DES, 3DES, IDEA or RC2 ciphers.

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
TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM

AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM

 3 POP3 Server Allows Plain Text Authentication Vulnerability port 110/tcp

QID:	74224
Category:	Mail services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/06/2008
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
Post Office Protocol version 3 (POP3) is an application layer internet standard protocol to retrieve e-mail from a remote server.
Use of the PASS command sends passwords in the clear over the network. Also, servers that answer -ERR to the User command are giving potential attackers clues about which names are valid.

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.

SOLUTION:
POP3 supports several authentication methods to provide varying levels of protection. Contact your vendor for further configuration information.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:
No results available

 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 (http://www.faqs.org/rfcs/rfc2554.html) and RFC 2487 (http://www.faqs.org/rfcs/rfc2487.html) 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-Hello qualysguard.com [1]
250-SIZE 20971520
250-8BITMIME
250-PIPELINING
250-AUTH PLAIN LOGIN
250-STARTTLS
250 HELP

AUTH LOGIN

334 VXNlcm5hbWU6

EHLO qualysguard.com

250-Hello qualysguard.com []
250-SIZE 20971520
250-8BITMIME
250-PIPELINING
250-AUTH PLAIN LOGIN
250-STARTTLS
250 HELP

AUTH PLAIN

334

3 Mail Server Accepts Plaintext Credentials port 587/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 (http://www.faqs.org/rfcs/rfc2554.html) and RFC 2487 (http://www.faqs.org/rfcs/rfc2487.html) 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-Hello qualysguard.com [1]
250-SIZE 20971520
250-8BITMIME
250-PIPELINING
250-AUTH PLAIN LOGIN
250-STARTTLS
250 HELP

AUTH LOGIN

334 VXNlcm5hbWU6

EHLO qualysguard.com

250- Hello qualysguard.com [1]
250-SIZE 20971520
250-8BITMIME
250-PIPELINING
250-AUTH PLAIN LOGIN
250-STARTTLS
250 HELP

AUTH PLAIN

334

3 SSL/TLS use of weak RC4 cipher port 110/tcp over SSL

QID:	38601
Category:	General remote services
CVE ID:	CVE-2013-2566, CVE-2015-2808
Vendor Reference:	-
Bugtraq ID:	91787, 58796, 73684
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS) protocols provide integrity, confidentiality and authenticity services to other protocols that lack these features.
SSL/TLS protocols use ciphers such as AES,DES, 3DES and RC4 to encrypt the content of the higher layer protocols and thus provide the confidentiality service. Normally the output of an encryption process is a sequence of random looking bytes. It was known that RC4 output has some bias in the output. Recently a group of researchers has discovered that the there is a stronger bias in RC4, which make statistical analysis of ciphertext more practical.
The described attack is to inject a malicious javascript into the victim's browser that would ensure that there are multiple connections being established with a target website and the same HTTP cookie is sent multiple times to the website in encrypted form. This provides the attacker a large set of ciphertext samples, that can be used for statistical analysis.
NOTE: On 3/12/15 NVD changed the CVSS v2 access complicity from high to medium. As a result Qualys revised the CVSS score to 4.3 immediately. On 5/4/15 Qualys is also revising the severity to level 3.

IMPACT:

If this attack is carried out and an HTTP cookie is recovered, then the attacker can use the cookie to impersonate the user whose cookie was recovered.
This attack is not very practical as it requires the attacker to have access to millions of samples of ciphertext, but there are certain assumptions that an attacker can make to improve the chances of recovering the cleartext from cihpertext. For examples HTTP cookies are either base64 encoded or hex digits. This information can help the attacker in their efforts to recover the cookie.

SOLUTION:

RC4 should not be used where possible. One reason that RC4 was still being used was BEAST and Lucky13 attacks against CBC mode ciphers in SSL and
TLS. However, TLSv 1.2 or later address these issues.

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
TLSv1 WITH RC4 CIPHERS IS SUPPORTED					
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED					
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED					

RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM

3 SSL/TLS Server supports TLSv1.0 port 110/tcp over SSL

QID:	38628
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/20/2018
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs.
For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.
RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack.
TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security.
A POODLE-type (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) attack could also be launched directly at TLS without negotiating a downgrade.
This QID is a PCI FAIL in accordance with the PCI standards.

Further details can be found under: PCI: Use of SSL Early TLS and ASV Scans (https://www.pcisecuritystandards.org/documents/Use-of-SSL-Early-TLS-and-ASV-Scans.pdf)

IMPACT:

An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications.
For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages.
A POODLE-type (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) attack could also be launched directly at TLS without negotiating a downgrade.

SOLUTION:

Disable the use of TLSv1.0 protocol in favor of a cryptographically stronger protocol such as TLSv1.2.
The following openssl commands can be used
to do a manual test:
openssl s_client -connect ip:port -tls1

If the test is successful, then the target support TLSv1

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.0 is supported

3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) port 110/tcp over SSL

QID:	38657

Category:	General remote services
CVE ID:	CVE-2016-2183
Vendor Reference:	-
Bugtraq ID:	92630, 95568
Service Modified:	05/30/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Legacy block ciphers having block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode.
All versions of SSL/TLS
protocol support cipher suites which use DES, 3DES, IDEA or RC2 as the symmetric encryption cipher are affected.

IMPACT:
Remote attackers can obtain cleartext data via a birthday attack against a long-duration encrypted session.

SOLUTION:
Disable and stop using DES, 3DES, IDEA or RC2 ciphers.

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
TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM

 3 SSL/TLS use of weak RC4 cipher port 143/tcp over SSL

QID:	38601
Category:	General remote services
CVE ID:	CVE-2013-2566, CVE-2015-2808
Vendor Reference:	-
Bugtraq ID:	91787, 58796, 73684

Service Modified: 01/29/2016
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS) protocols provide integrity, confidentiality and authenticity services to other protocols that lack these features.
SSL/TLS protocols use ciphers such as AES,DES, 3DES and RC4 to encrypt the content of the higher layer protocols and thus provide the confidentiality service. Normally the output of an encryption process is a sequence of random looking bytes. It was known that RC4 output has some bias in the output. Recently a group of researchers has discovered that the there is a stronger bias in RC4, which make statistical analysis of ciphertext more practical.
The described attack is to inject a malicious javascript into the victim's browser that would ensure that there are multiple connections being established with a target website and the same HTTP cookie is sent multiple times to the website in encrypted form. This provides the attacker a large set of ciphertext samples, that can be used for statistical analysis.
NOTE: On 3/12/15 NVD changed the CVSS v2 access complicity from high to medium. As a result Qualys revised the CVSS score to 4.3 immediately. On 5/4/15 Qualys is also revising the severity to level 3.

IMPACT:

If this attack is carried out and an HTTP cookie is recovered, then the attacker can use the cookie to impersonate the user whose cookie was recovered.
This attack is not very practical as it requires the attacker to have access to millions of samples of ciphertext, but there are certain assumptions that an attacker can make to improve the chances of recovering the cleartext from cihpertext. For examples HTTP cookies are either base64 encoded or hex digits. This information can help the attacker in their efforts to recover the cookie.

SOLUTION:

RC4 should not be used where possible. One reason that RC4 was still being used was BEAST and Lucky13 attacks against CBC mode ciphers in SSL and
TLS. However, TLSv 1.2 or later address these issues.

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
TLSv1 WITH RC4 CIPHERS IS SUPPORTED					
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED					
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED					
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM

 3 SSL/TLS Server supports TLSv1.0 port 143/tcp over SSL

QID: 38628

Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/20/2018
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs.
For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.
RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack.
TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security.
A POODLE-type (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) attack could also be launched directly at TLS without negotiating a downgrade.
This QID is a PCI FAIL in accordance with the PCI standards.

Further details can be found under: PCI: Use of SSL Early TLS and ASV Scans (https://www.pcisecuritystandards.org/documents/Use-of-SSL-Early-TLS-and-ASV-Scans.pdf)

IMPACT:

An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications.
For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages.
A POODLE-type (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) attack could also be launched directly at TLS without negotiating a downgrade.

SOLUTION:

Disable the use of TLSv1.0 protocol in favor of a cryptographically stronger protocol such as TLSv1.2.
The following openssl commands can be used
to do a manual test:
openssl s_client -connect ip:port -tls1

If the test is successful, then the target support TLSv1

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.0 is supported

3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) port 143/tcp over SSL

QID:	38657
Category:	General remote services
CVE ID:	CVE-2016-2183
Vendor Reference:	-
Bugtraq ID:	92630, 95568
Service Modified:	05/30/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Legacy block ciphers having block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode.
All versions of SSL/TLS
protocol support cipher suites which use DES, 3DES, IDEA or RC2 as the symmetric encryption cipher are affected.

IMPACT:
Remote attackers can obtain cleartext data via a birthday attack against a long-duration encrypted session.

SOLUTION:
Disable and stop using DES, 3DES, IDEA or RC2 ciphers.

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
TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM

 3 SSL/TLS use of weak RC4 cipher port 25/tcp over SSL

QID:	38601
Category:	General remote services
CVE ID:	CVE-2013-2566, CVE-2015-2808
Vendor Reference:	-
Bugtraq ID:	91787, 58796, 73684
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS) protocols provide integrity, confidentiality and authenticity services to other

protocols that lack these features.
SSL/TLS protocols use ciphers such as AES,DES, 3DES and RC4 to encrypt the content of the higher layer protocols and thus provide the confidentiality service. Normally the output of an encryption process is a sequence of random looking bytes. It was known that RC4 output has some bias in the output. Recently a group of researchers has discovered that the there is a stronger bias in RC4, which make statistical analysis of ciphertext more practical.
The described attack is to inject a malicious javascript into the victim's browser that would ensure that there are multiple connections being established with a target website and the same HTTP cookie is sent multiple times to the website in encrypted form. This provides the attacker a large set of ciphertext samples, that can be used for statistical analysis.
NOTE: On 3/12/15 NVD changed the CVSS v2 access complicity from high to medium. As a result Qualys revised the CVSS score to 4.3 immediately. On 5/4/15 Qualys is also revising the severity to level 3.

IMPACT:

If this attack is carried out and an HTTP cookie is recovered, then the attacker can use the cookie to impersonate the user whose cookie was recovered.
This attack is not very practical as it requires the attacker to have access to millions of samples of ciphertext, but there are certain assumptions that an attacker can make to improve the chances of recovering the cleartext from cihpertext. For examples HTTP cookies are either base64 encoded or hex digits. This information can help the attacker in their efforts to recover the cookie.

SOLUTION:

RC4 should not be used where possible. One reason that RC4 was still being used was BEAST and Lucky13 attacks against CBC mode ciphers in SSL and
TLS. However, TLSv 1.2 or later address these issues.

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
TLSv1 WITH RC4 CIPHERS IS SUPPORTED					
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED					
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED					
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM

3 SSL/TLS Server supports TLSv1.0

port 25/tcp over SSL

QID:	38628
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/20/2018
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs.
For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.
RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack.
TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security.
A POODLE-type (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) attack could also be launched directly at TLS without negotiating a downgrade.
This QID is a PCI FAIL in accordance with the PCI standards.

Further details can be found under: PCI: Use of SSL Early TLS and ASV Scans (https://www.pcisecuritystandards.org/documents/Use-of-SSL-Early-TLS-and-ASV-Scans.pdf)

IMPACT:

An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications.
For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages.
A POODLE-type (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) attack could also be launched directly at TLS without negotiating a downgrade.

SOLUTION:

Disable the use of TLSv1.0 protocol in favor of a cryptographically stronger protocol such as TLSv1.2.
The following openssl commands can be used
to do a manual test:
openssl s_client -connect ip:port -tls1

If the test is successful, then the target support TLSv1

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.0 is supported

3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) port 25/tcp over SSL

QID:	38657
Category:	General remote services
CVE ID:	CVE-2016-2183
Vendor Reference:	-
Bugtraq ID:	92630, 95568
Service Modified:	05/30/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Legacy block ciphers having block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode.
All versions of SSL/TLS
protocol support cipher suites which use DES, 3DES, IDEA or RC2 as the symmetric encryption cipher are affected.

IMPACT:

Remote attackers can obtain cleartext data via a birthday attack against a long-duration encrypted session.

SOLUTION:

Disable and stop using DES, 3DES, IDEA or RC2 ciphers.

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
TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM

3 SSL/TLS use of weak RC4 cipher

port 587/tcp over SSL

QID:	38601
Category:	General remote services
CVE ID:	CVE-2013-2566, CVE-2015-2808
Vendor Reference:	-
Bugtraq ID:	91787, 58796, 73684
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS) protocols provide integrity, confidentiality and authenticity services to other protocols that lack these features.
SSL/TLS protocols use ciphers such as AES,DES, 3DES and RC4 to encrypt the content of the higher layer protocols and thus provide the confidentiality service. Normally the output of an encryption process is a sequence of random looking bytes. It was known that RC4 output has some bias in the output. Recently a group of researchers has discovered that the there is a stronger bias in RC4, which make statistical analysis of ciphertext more practical.
The described attack is to inject a malicious javascript into the victim's browser that would ensure that there are multiple connections being established with a target website and the same HTTP cookie is sent multiple times to the website in encrypted form. This provides the attacker a large set of ciphertext samples, that can be used for statistical analysis.
NOTE: On 3/12/15 NVD changed the CVSS v2 access complicity from high to medium. As a result Qualys revised the CVSS score to 4.3 immediately. On 5/4/15 Qualys is also revising the severity to level 3.

IMPACT:
If this attack is carried out and an HTTP cookie is recovered, then the attacker can use the cookie to impersonate the user whose cookie was recovered.
This attack is not very practical as it requires the attacker to have access to millions of samples of ciphertext, but there are certain assumptions that

an attacker can make to improve the chances of recovering the cleartext from cihpertext. For examples HTTP cookies are either base64 encoded or hex digits. This information can help the attacker in their efforts to recover the cookie.

SOLUTION:
RC4 should not be used where possible. One reason that RC4 was still being used was BEAST and Lucky13 attacks against CBC mode ciphers in SSL and
TLS. However, TLSv 1.2 or later address these issues.

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
TLSv1 WITH RC4 CIPHERS IS SUPPORTED					
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED					
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED					
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM

3 SSL/TLS Server supports TLSv1.0 port 587/tcp over SSL

QID:	38628
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/20/2018
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs.
For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.
RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack.
TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security.
A POODLE-type (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) attack could also be launched directly at TLS without negotiating a downgrade.
This QID is a PCI FAIL in accordance with the PCI standards.

Further details can be found under: PCI: Use of SSL Early TLS and ASV Scans (https://www.pcisecuritystandards.org/documents/Use-of-SSL-Early-TLS-and-ASV-Scans.pdf)

IMPACT:
An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications.
For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages.
A POODLE-type (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) attack could also be launched directly at TLS without negotiating a downgrade.

SOLUTION:
Disable the use of TLSv1.0 protocol in favor of a cryptographically stronger protocol such as TLSv1.2.
The following openssl commands can be used
to do a manual test:
openssl s_client -connect ip:port -tls1

If the test is successful, then the target support TLSv1

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:
TLSv1.0 is supported

3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) port 587/tcp over SSL

QID:	38657
Category:	General remote services
CVE ID:	CVE-2016-2183
Vendor Reference:	-
Bugtraq ID:	92630, 95568
Service Modified:	05/30/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Legacy block ciphers having block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode.
All versions of SSL/TLS
protocol support cipher suites which use DES, 3DES, IDEA or RC2 as the symmetric encryption cipher are affected.

IMPACT:
Remote attackers can obtain cleartext data via a birthday attack against a long-duration encrypted session.

SOLUTION:
Disable and stop using DES, 3DES, IDEA or RC2 ciphers.

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

TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM

 3 SSL/TLS use of weak RC4 cipher port 993/tcp over SSL

QID:	38601
Category:	General remote services
CVE ID:	CVE-2013-2566, CVE-2015-2808
Vendor Reference:	-
Bugtraq ID:	91787, 58796, 73684
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS) protocols provide integrity, confidentiality and authenticity services to other protocols that lack these features.
SSL/TLS protocols use ciphers such as AES,DES, 3DES and RC4 to encrypt the content of the higher layer protocols and thus provide the confidentiality service. Normally the output of an encryption process is a sequence of random looking bytes. It was known that RC4 output has some bias in the output. Recently a group of researchers has discovered that the there is a stronger bias in RC4, which make statistical analysis of ciphertext more practical.
The described attack is to inject a malicious javascript into the victim's browser that would ensure that there are multiple connections being established with a target website and the same HTTP cookie is sent multiple times to the website in encrypted form. This provides the attacker a large set of ciphertext samples, that can be used for statistical analysis.
NOTE: On 3/12/15 NVD changed the CVSS v2 access complicity from high to medium. As a result Qualys revised the CVSS score to 4.3 immediately. On 5/4/15 Qualys is also revising the severity to level 3.

IMPACT:

If this attack is carried out and an HTTP cookie is recovered, then the attacker can use the cookie to impersonate the user whose cookie was recovered.
This attack is not very practical as it requires the attacker to have access to millions of samples of ciphertext, but there are certain assumptions that an attacker can make to improve the chances of recovering the cleartext from cihpertext. For examples HTTP cookies are either base64 encoded or hex digits. This information can help the attacker in their efforts to recover the cookie.

SOLUTION:

RC4 should not be used where possible. One reason that RC4 was still being used was BEAST and Lucky13 attacks against CBC mode ciphers in SSL and
TLS. However, TLSv 1.2 or later address these issues.

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
TLSv1 WITH RC4 CIPHERS IS SUPPORTED					
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED					
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED					
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM

3 SSL/TLS Server supports TLSv1.0

port 993/tcp over SSL

QID:	38628
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/20/2018
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs.
For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.
RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack.
TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security.
A POODLE-type (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) attack could also be launched directly at TLS without negotiating a downgrade.
This QID is a PCI FAIL in accordance with the PCI standards.

Further details can be found under: PCI: Use of SSL Early TLS and ASV Scans (https://www.pcisecuritystandards.org/documents/Use-of-SSL-Early-TLS-and-ASV-Scans.pdf)

IMPACT:
An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications.
For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages.
A POODLE-type (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) attack could also be launched directly at TLS without negotiating a downgrade.

SOLUTION:
Disable the use of TLSv1.0 protocol in favor of a cryptographically stronger protocol such as TLSv1.2.
The following openssl commands can be used

to do a manual test:
openssl s_client -connect ip:port -tls1

If the test is successful, then the target support TLSv1

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:
TLSv1.0 is supported

3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) port 993/tcp over SSL

QID:	38657
Category:	General remote services
CVE ID:	CVE-2016-2183
Vendor Reference:	-
Bugtraq ID:	92630, 95568
Service Modified:	05/30/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Legacy block ciphers having block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode.
All versions of SSL/TLS
protocol support cipher suites which use DES, 3DES, IDEA or RC2 as the symmetric encryption cipher are affected.

IMPACT:
Remote attackers can obtain cleartext data via a birthday attack against a long-duration encrypted session.

SOLUTION:
Disable and stop using DES, 3DES, IDEA or RC2 ciphers.

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
TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM

ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM

3 SSL/TLS use of weak RC4 cipher

port 995/tcp over SSL

QID:	38601
Category:	General remote services
CVE ID:	CVE-2013-2566, CVE-2015-2808
Vendor Reference:	-
Bugtraq ID:	91787, 58796, 73684
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS) protocols provide integrity, confidentiality and authenticity services to other protocols that lack these features.
SSL/TLS protocols use ciphers such as AES,DES, 3DES and RC4 to encrypt the content of the higher layer protocols and thus provide the confidentiality service. Normally the output of an encryption process is a sequence of random looking bytes. It was known that RC4 output has some bias in the output. Recently a group of researchers has discovered that the there is a stronger bias in RC4, which make statistical analysis of ciphertext more practical.
The described attack is to inject a malicious javascript into the victim's browser that would ensure that there are multiple connections being established with a target website and the same HTTP cookie is sent multiple times to the website in encrypted form. This provides the attacker a large set of ciphertext samples, that can be used for statistical analysis.
NOTE: On 3/12/15 NVD changed the CVSS v2 access complicity from high to medium. As a result Qualys revised the CVSS score to 4.3 immediately. On 5/4/15 Qualys is also revising the severity to level 3.

IMPACT:

If this attack is carried out and an HTTP cookie is recovered, then the attacker can use the cookie to impersonate the user whose cookie was recovered.
This attack is not very practical as it requires the attacker to have access to millions of samples of ciphertext, but there are certain assumptions that an attacker can make to improve the chances of recovering the cleartext from cihpertext. For examples HTTP cookies are either base64 encoded or hex digits. This information can help the attacker in their efforts to recover the cookie.

SOLUTION:

RC4 should not be used where possible. One reason that RC4 was still being used was BEAST and Lucky13 attacks against CBC mode ciphers in SSL and
TLS. However, TLSv 1.2 or later address these issues.

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
TLSv1 WITH RC4 CIPHERS IS SUPPORTED					
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM

TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED					
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED					
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM

3 SSL/TLS Server supports TLSv1.0 port 995/tcp over SSL

QID:	38628
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/20/2018
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs.
For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.
RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack.
TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security.
A POODLE-type (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) attack could also be launched directly at TLS without negotiating a downgrade.
This QID is a PCI FAIL in accordance with the PCI standards.

Further details can be found under: PCI: Use of SSL Early TLS and ASV Scans (https://www.pcisecuritystandards.org/documents/Use-of-SSL-Early-TLS-and-ASV-Scans.pdf)

IMPACT:

An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications.
For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages.
A POODLE-type (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) attack could also be launched directly at TLS without negotiating a downgrade.

SOLUTION:

Disable the use of TLSv1.0 protocol in favor of a cryptographically stronger protocol such as TLSv1.2.
The following openssl commands can be used
to do a manual test:
openssl s_client -connect ip:port -tls1

If the test is successful, then the target support TLSv1

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.0 is supported

3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) port 995/tcp over SSL

QID:	38657
Category:	General remote services
CVE ID:	CVE-2016-2183
Vendor Reference:	-
Bugtraq ID:	92630, 95568
Service Modified:	05/30/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Legacy block ciphers having block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode.
All versions of SSL/TLS
protocol support cipher suites which use DES, 3DES, IDEA or RC2 as the symmetric encryption cipher are affected.

IMPACT:

Remote attackers can obtain cleartext data via a birthday attack against a long-duration encrypted session.

SOLUTION:

Disable and stop using DES, 3DES, IDEA or RC2 ciphers.

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
TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM

2 AutoComplete Attribute Not Disabled for Password in Form Based Authentication port 443/tcp

QID:	86729
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/11/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Web server allows form based authentication without disabling the AutoComplete feature for the password field.
Autocomplete should be turned off for any input that takes sensitive information such as credit card number, CVV2/CVC code, U.S. social security number, etc.

IMPACT:

If the browser is used in a shared computing environment where more than one person may use the browser, then "autocomplete" values may be retrieved or submitted by an unauthorized user.

SOLUTION:

Contact the vendor to have the AutoComplete attribute disabled for the password field in all forms. The AutoComplete attribute should also be disabled for the user ID field.
Developers can add the following attribute to the form or input element: autocomplete="off"
This attribute prevents the browser from prompting the user to save the populated form values for later reuse.
Most browsers no longer honor autocomplete="off" for password input fields. These browsers include Chrome, Firefox, Microsoft Edge, IE, Opera
However, there is still an ability to turn off autocomplete through the browser and that is recommended for a shared computing environment.
Since the ability to turn autocomplete off for password inputs fields is controlled by the user it is highly recommended for application to enforce strong password rules.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

GET /wp-login.php HTTP/1.0
Host: Name
<input type="hidden" name="testcookie" value="1" />
</p>
</form>

2 SSL Certificate - Expired port 465/tcp over SSL

QID:	38167

Appendix

Hosts Scanned (IP)

Target distribution across scanner appliances

Hosts Not Scanned

Hosts Not Alive (IP) (4)

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:	Disabled
Oracle:	Disabled
Oracle Listener:	Disabled
SNMP:	Disabled
VMware:	Disabled
DB2:	Disabled
HTTP:	Disabled
MySQL:	Disabled
Tomcat Server:	Disabled
MongoDB:	Disabled
Palo Alto Networks Firewall:	Disabled
Jboss Server:	Disabled
Oracle WebLogic Server:	Disabled
MariaDB:	Disabled
Overall Performance:	Normal
Authenticated Scan Certificate Discovery:	Disabled
Test Authentication:	Disabled

Hosts to Scan in Parallel:	
Use Appliance Parallel ML Scaling:	Off
External Scanners:	15
Scanner Appliances:	30
Processes to Run in Parallel:	
Total Processes:	10
HTTP Processes:	10
Packet (Burst) Delay:	Medium
Port Scanning and Host Discovery:	
Intensity:	Normal
Dissolvable Agent:	
Dissolvable Agent (for this profile):	Disabled
Windows Share Enumeration:	Disabled
Windows Directory Search:	Disabled
Lite OS Discovery:	Disabled
Host Alive Testing:	Disabled
Do Not Overwrite OS:	Disabled

Advanced Settings

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

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.