

Process Owner: IT Operations	FORM	F-CMG-3.1
	<i>Securing SSLProtocol and CipherSuite</i>	

Request Information				
Requestor	Alvinn Medrano			
Implementing Team	Server Operation			
Ticket Number/s				
Change Classification		Major	x	Minor
After the fact	x	Yes		No
Emergency		Yes	x	No
Proposed Change Date	ATF			
Proposed Change Start/End Time	ATF			
Proposed Change Verification Time	ATF			

Objective of the change
To ensures that a connection to a remote endpoint is securely encrypted in order to provide privacy and data integrity.

Technical/Operational Impact of the change		
Negative: No negative impact to the production.	Beneficial: Server encryption level has been strengthened.	Neutral: Compliance with PCIDSS requirements.

Affected IT Infrastructure components			
Site	Hostname	IP Address	Function
Jaka	<ul style="list-style-type: none"> JKA-VWIN-WSUS01 OSTicket JKA-VWIN-DC01 	<ul style="list-style-type: none"> 172.17.0.123 172.17.0.3 172.17.0.121 	<ul style="list-style-type: none"> WSUS server Logging and Ticketing Server AD server
G2	<ul style="list-style-type: none"> GL2-VWIN-DC01 GL2-VWIN-DC02 GL2-VLIN-NMS01 	<ul style="list-style-type: none"> 172.22.1.1 172.22.9.4 172.22.1.2 	<ul style="list-style-type: none"> Primary AD server Secondary AD server Monitoring server

Affected Departments and corresponding contact persons		
Department	Contact Name	Contact Info
Server Operation	Rovie Salvatiera	0917-627-4325

Test Environment implementation and Verification Summary
No testing as it was an after the fact.

Test Environment Results Summary
No testing as it was an after the fact.

Process Owner: IT Operations	FORM	F-CMG-3.1
	<i>Securing SSLProtocol and CipherSuite</i>	

Configuration Change Template

Baseline File	3.1.154 JKA-VWIN-WSUS01, 3.1.124 OSTicket, 3.1.145 JKA-VWIN-DC01, 3.1.140 NETWORK & SYSTEM MONITORING, 3.1.137 DOMAIN FOREST
Baseline Version	2.0

Baseline File Changes:

Existing Configuration	Proposed Change	Impact	Section
The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0.	Disable TLS 1.0 SSL 2.0 and 3.0 and enforced higher encryption using TLS 1.2 or above	Add new file tab for Encryption level	Encryption Level

Physical Implementation Procedures / Advisory

No physical implementation will be facilitated.

Backup Procedures


Windows Servers

1. Login into the servers using your own admin account
2. Type regedit in the search box
3. Click regedit from the search results list
4. Click Yes, if you're prompted by User Account Control
5. Select Computer from the left side. Make sure it's selected before you proceed to the next step.
6. Go to File and then click on Export
7. At the Export Registry File, type a name for the backup file
8. Choose All under the Export range section
9. Select a location where you want to save the backup file
10. Click Save

Linux Servers

1. Login via SSH in the linux server using your own credentials
2. Go to /etc/httpd/conf.d
3. Then type cp /etc/httpd/conf.d/ssl.conf /etc/httpd/conf.f/ssl.conf.bak

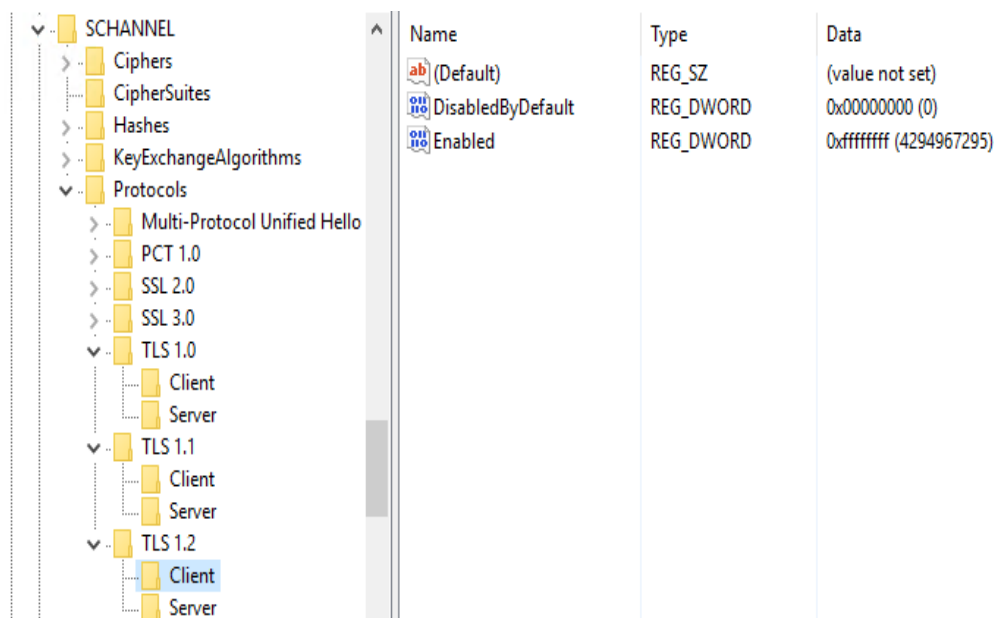
Technical Configuration Procedures

	Proprietary and Confidential	Effectivity: April 1, 2019	Page 2
			Template Version : 02

Process Owner: IT Operations	FORM	F-CMG-3.1
	<i>Securing SSLProtocol and CipherSuite</i>	

Windows Servers

1. Login into the servers using your own admin account
2. Hit Windows + Run and type regedit in the search box
3. Go to >HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Control > SecurityProviders > SCHANNEL
4. Select "Protocol" then set TLS 1.0 and 1.1 enabled value to 1 to disable.
5. Select TLS 1.2 and set the value to 0 to enable




Linux Servers

1. Login to Linux Server via SSH using your own root credentials
2. Type vi / etc/httpd/conf.d/ssl.conf to edit current ssl config

```
[root@osticket conf.d]# pwd
/etc/httpd/conf.d
[root@osticket conf.d]# ll
total 32
-rw-r--r-- 1 root root 674 Mar 22 2017 php.conf
-rw-r--r-- 1 root root 1751 Dec 15 2016 phpMyAdmin.conf
-rw-r--r-- 1 root root 1744 Dec 15 2016 phpMyAdmin.conf.rpmsave
-rw-r--r-- 1 root root 392 Jun 19 2018 README
-rw-r--r-- 1 root root 9705 May 14 18:51 ssl.conf
-rw-r--r-- 1 root root 299 Feb 19 2018 welcome.conf
[root@osticket conf.d]#
```

3. Edit SSLProtocol and SSLCipherSuite and copy values below.

SSLCipherSuite

 OPEN ACCESS	Proprietary and Confidential	Effectivity: April 1, 2019	Page 3
			Template Version : 02

Process Owner: IT Operations	FORM	F-CMG-3.1
	<i>Securing SSLProtocol and CipherSuite</i>	

- SSLCipherSuite ECDH+AES:EDH+AES:-SHA1:EECDH+RC4:EDH+RC4:RC4-SHA:EECDH+AES256:EDH+AES256:AES256-SHA:!aNULL:!eNULL:!EXP:!MEDIUM:!LOW:!MD5

SSLProtocol

- SSLProtocol -ALL +TLSv1.2

```
SSLProtocol -ALL +TLSv1.2

# SSL Cipher Suite:
# List the ciphers that the client is permitted to negotiate
# See the mod_ssl documentation for a complete list.
# SSLCipherSuite HIGH:MEDIUM:!aNULL:!MD5:!SEED:!IDEA
#SSLCipherSuite HIGH:!aNULL:!MD5
SSLCipherSuite ECDH+AES:EDH+AES:-SHA1:EECDH+RC4:EDH+RC4:RC4-SHA:EECDH+AES256:EDH+AES256:AES256-SHA:!aNULL:!eNULL:!EXP:!MEDIUM:!LOW:!MD5
#SSLHonorCipherOrder on
#SSLCompression Off
```

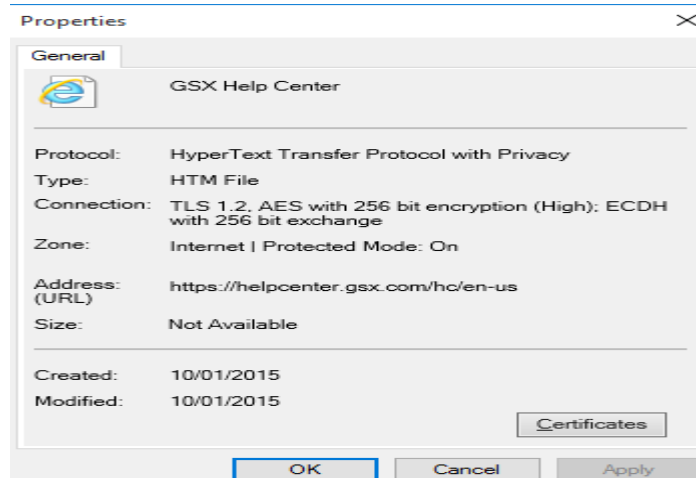
4. Hit esc + :wq! to save the file config
5. Restart HTTP service type service httpd restart.

Verification Procedures

1. Run Nessus network scanner in server with affected issue with TLS and SSL is already solved.

Windows Servers

1. Launch Internet Explorer.
2. Enter the URL you wish to check in the browser.
3. Right-click the page or select the Page drop-down menu and select Properties.
4. In the new window, look for the Connection section. This will describe the version of TLS or SSL used.



Linux Servers

1. Login to server via SSH
2. openssl s_client -connect localhost:443 -ssl2 or -ssl3 or tls1_1

Process Owner: IT Operations	FORM	F-CMG-3.1
	<i>Securing SSLProtocol and CipherSuite</i>	

3. If it shows an error like SSL2_WRITE:ssl handshake failure:s2_pkt.c, it means SSL v2.0 has been disabled.

```
[root@osticket conf.d]# openssl s_client -connect localhost:443 -tls1_1
CONNECTED (00000003)
139724384929608:error:1409442E:SSL routines:SSL3_READ_BYTES:tlsv1 alert protocol version:s3_pkt.c:1275:SSL alert number 70
139724384929608:error:1409E0E5:SSL routines:SSL3_WRITE_BYTES:ssl handshake failure:s3_pkt.c:598:
---
no peer certificate available
```

Back-out Procedures

Windows Servers

1. Login into the servers using your own admin account
2. Open the Registry Editor: type regedit at the search box and click on the regedit item when it appears in the search results list.
3. At File, click the Import option
4. At the Import Registry File screen, browse and select the backup file you want to restore
5. Click Open

Linux Servers

1. Login via SSH in the linux server using your own credentials
2. Go to /etc/httpd/conf.d
3. Remove ssl.conf type "rm ssl.conf"
4. Then type cp /etc/httpd/conf.d/ssl.conf.bak /etc/httpd/conf.f/ssl.conf to restore old config.