# UCCE 12.5のセキュリティ強化について

### 内容

概要 <u>前提条件</u> <u>要件</u> <u>使用するコンポーネント</u> <u>背景説明</u> <u>ダウンロードしたISOの確認</u> <u>SHA-256およびキーサイズ2048ビットの証明書の使用</u> <u>SSLUtilツール</u> <u>DiagFwCertMgrコマンド</u> データ保護ツール

### 概要

このドキュメントでは、Unified Contact Center Enterprise(UCCE)12.5で追加された最新のセキュ リティ拡張機能について説明します。

# 前提条件

- UCCE
- SSL (Open Secure Sockets Layer)

### 要件

次の項目に関する知識があることが推奨されます。

• UCCE 12.5

•オープンSSL

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

• UCCE 12.5

• Windows用OpenSSL(64ビット)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく ださい。

## 背景説明

Cisco Security Control Framework(SCF):Collaboration Security Control Frameworkは、セキュア で信頼性の高いコラボレーションインフラストラクチャを構築するための設計および実装ガイド ラインを提供します。これらのインフラストラクチャは、既知の攻撃と新しい攻撃の両方に対し て復元力があります。Cisco <u>Unified ICM/Contact Center Enterpriseリリース12.5のセキュリティ</u> <u>ガイドを参照してください</u>。

シスコのSCFの取り組みの一環として、UCCE 12.5に追加されたセキュリティ強化が加えられました。このドキュメントでは、これらの強化の概要について説明します。

# ダウンロードしたISOの確認

シスコによって署名されたダウンロード済みISOを検証し、承認されていることを確認するには 、次の手順を実行します。

1. OpenSSLのダウンロードとインストールソフトウェア「openssl softpedia」を検索します。

SOFTPEDIA		C DRIVERS	co GAMES	C NAC	ANDROID APK	🛎 LINUX	IN NEWS & REVIEW	is 🎈 🕯	4
Sofipelia > Windows	> Programming > Component	s & Ubrarles > 0	iperSil.		IREE TRUST, 📥 Dee	ver Booster	6 FRO (60% OFF w	hen you buy	yî.
Advertisement									Ξ
OpenSSL							Search		a,
								_	-

2.**パス**を確認します(これはデフォルトで設定されますが、検証には有効です)。 Windows 10で は、[システムプロパティ]に移動し、[環境変数]を選択します。

Edit System Variable	_	×
Variable name: OPENSS	L_CONF	
Variable value: CAOper	hSSL-Win64\bin\openssl.cfg	
Browse Directory	Browse File	OK Cancel
JAVA_HOME JAVA_OPTS NUMBER_OF_PROCESSORS	C:\Program Files (x86)\Java\jre1.8.0_221 -Dbundle.provider.className=com.cisco.c 6	cbu.cce.cceadmin.i18n
OPENSSL_CONF OS	C:\OpenSSL-Win64\bin\openssl.cfg Windows_NT	

3. ISO検証に必要なファイル

	>	This	PC > Local Disk (C:) > ISO	5 ~	Search ISO	ېر
		^	Name	Date modified	Туре	Size
55			CCEInst1251	2/24/2020 2:31 PM	WinRAR archive	1,129,294 KB
	ж		CCEInst1251.iso.md5	2/24/2020 2:27 PM	MD5 File	1 KB
is	A		CCEInst1251.iso.signature	2/24/2020 2:27 PM	SIGNATURE File	1 KB
ts	A		🔄 UCCEReleaseCodeSign_pubkey	2/24/2020 2:27 PM	Security Certificate	1 KB

#### 4.コマンドラインからOpenSSLツールを実行します。



#### 5. 次のコマンドを実行します。

dgst -sha512 -keyform der -verify <public Key.der> -signature <ISO image.iso.signature> <ISO Image>

#### 6.障害が発生した場合、コマンドラインにエラーが表示されます(図を参照)

OpenSSL> dgst -sha512 -keyform der -verify c:\iso\UCCEReleaseCodeSign\_pubkey.der -signature c:\iso\CCEInst1251.iso.signa ture c:\iso\CCEInst1251.iso Verification Failure error in dgst OpenSSL>

# SHA-256およびキーサイズ2048ビットの証明書の使用

ログは、非準拠の証明書を特定した場合にエラーを報告します(SHA-256またはキーサイズ 2048ビットの要件を満たしていない場合)。

UCCEの観点からは、次の2つの重要な証明書があります。

- Cisco ICM Diagnostic Frameworkサービス証明書
- Cisco ICM SSL証明書

証明書は、Windowsサーバのインターネットインフォメーションサービス(IIS)マネージャオプションで確認できます。



自己署名証明書(プロファイルの診断またはWebセットアップ用)の場合、次のエラー行が報告 されます。

Re-generating Cisco ICM SSL Certificate with SHA-256 and key size '2048' and will be binded with port 443.

#### SSLUtilツール

**a.**自己署名証明書(WebSetup/CCEAdminページ用)を再生成するには、SSLUtilツール(場所 C:\icm\bin)を使用します。

**b.**[Uninstall]を選択して、現在の[Cisco ICM SSL Certificate]を削除します。

🔕 SSL Encryption Utility	-		x				
File Help							
Configuration Certificate Administration							
Click Uninstall to remove the SSL certificate with the following thumbprint from IIS:							
8f 5b f5 52 d5 9e 4b 1d fe 18 e3 9d 47 f4 14 ee 24 57 1d cc							
Uninstall							
[Information] [SSLUtil] SSL Port already at "443" for IIS			_				
[Information] [SSLUtil] Number of instances: 1 [Information] [SSLUtil] instance[0]: pin12							
[Information] [SSLUtil] adding instance pin12 with app count of 1							
[Information] [SSLUtil] SSL is enabled for pin12->ise->pin12_scriptmon							
[Information] [SSLUtil] Comparing input: C:\icm\ssl\cfg\server-iis.xml output: C:\i [Information] [SSLUtil] Compare0 files are the same	icm \tomca	at \conf \se	rvero				
[Information] [SSLUtil] SSL is not enabled for common->setup->jakarta							
<			>				
Clear		Close					

**c.次に**Install in SSLUtilツールを選択し、プロセスが完了したら、作成された証明書にSHA-256ビ ットとkeysize '2048'ビットが含まれていることを確認します。

	💀 Certificate	ĸ
Server Certificates	General Details Certification Path	
Use this feature to request and manage certificates that the Web serv	Show: <all></all>	
Filter: 🔹 🤝 Go 🦂 🔤 Show All 🛛 Group by:	Field Value	
Name Issued To Cisco ICM Diagnostic Framew aw12.samaira.com Cisco ICM SSL Certificate aw12.samaira.com	Signature algorithm sha256RSA Signature hash algorithm sha256 Signature hash algorithm sha256 Sugnature hash algorithm sha256 Nonday, March 21, 2039 2:50 Subject aw12.samaira.com Public key RSA (2048 Bits)	
	Public key parameters 05 00	

### DiagFwCertMgrコマンド

Cisco ICM Diagnostic Frameworkサービス証明書の自己署名証明書を再生成するには、次の図に

示すように、コマンドライン「DiagFwCertMgr」を使用します。

C:\icm\serviceability\diagnostics\bin>DiagFwCertMgr /task:CreateAndBindCert

Executing Task: 'CreateAndBindCert'

Deleted old binding successfully Binding new certificate with HTTP service completed successfully Found existing registry key for the service Hash of certificate used saved in the service registry ALL TASKS FOR BINDING THE CERTIFICATE WITH HTTP SERVICE COMPLETED SUCCESSFULLY

C:\icm\serviceability\diagnostics\bin>\_

# データ保護ツール

1. CEDataProtectToolは、Windowsレジストリが格納する機密情報を暗号化および復号化するために使用されます。SQL 12.5へのアップグレード後、SQLLoginレジストリの値ストアを CEDataProtectToolで再構成する必要があります。このツールを実行できるのは、管理者権限を 持つ管理者、ドメインユーザー、またはローカル管理者のみです。

2.このツールは、SQLLoginレジストリの暗号化された値ストアの表示、構成、編集、削除に**使用** できます。

3.ツールは場所にあります。

<Install Directory>:\icm\bin\CCEDataProtectTool.exe 4.場所に移動し、[CEDataProtectTool.exe]をダブルクリックします。

File Home	Share	View Manage				~ 📀
← → ▼ ↑ 📘	→ Thi	s PC > Local Disk (C:) > icm > bin		✓ ♂ Search bir	ı	٩
		Name	Date modified	Туре	Size	^
📌 Quick access	1	CCEDataProtectTool	(7/2020 3:37 PM	Application	54 KB	
👆 Downloads	*	🛎 ccisCommon	12/19/2019 7:47 AM	Executable Jar File	1,403 KB	
📃 Desktop	1	📄 cdbin.ba_	12/19/2019 7:48 AM	BA_ File	1 KB	
Documents	*	s cdbin	4/18/2020 11:50 PM	Windows Batch File	1 KB	

5.暗号化するには、[DBLookup]に1を押し、[Instance Name]を入力します。次に、2を押して[Edit and Encrypt]を選択します

C:\icm\bin\CCEDataProtectTool.exe CCEDataProtectTool supports Encryption/Decryption of sensitive information in Windows Registry. Nain Menu: Select one of the below options 1. DBLookup <del> </del>2. Rekey Help 4. Exit Enter Instance Name: cc125 Select one of the below options for DBLookup Registry 4. Exit Fetching / Decryption failed, Refer the C:\temp\CCEDataProtect.log for more Details Enter New Registry Value: Are you sure you want to Edit the Registry Details [Y/N] Registry Updated with Encrypted Data Successfully. Select one of the below options for DBLookup Registry Help . Decrypt and View Edit and Encrypt 4. Exit

6.レジストリの場所に移動し、「文字列値SQLLoginが空のように表示されます(図を参照)。

HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems,					
Inc.\ICM\pini2\Routera\I	Router (Currentversion)	Configuration (Database			
Name	Туре	Data			
(Default)	REG_SZ	(value not set)			
R Abandon Timeout	REG DWORD	0x00001388 (5000)			
ab SQLLogin	REG_SZ				
ug Inreads	REG_DWORD	0x0000005 (5)			
80 Timeout	REG_DWORD	0x0000015e (350)			
Edit String		×			
Value name:					
SQLLogin					
Value data:					
		OK Cancel			

(7)暗号化値の確認が必要な場合図に示すように、CEDataProtectToolのコマンドラインで、 [Decrypt and View]に1を選択します。



### 8.このツールのログは、場所にあります。

<Install Directory>:\temp

Audit logs filename : CCEDataProtectTool\_Audit CCEDataProtectTool logs : CCEDataProtectTool

	> This	PC > Local Disk (Ci) > Temp >	~	Search Temp	Q
		Name	Date modified	Туре	Size
-55		🖹 CCEDataProtectTooLAudit ←	3/5/2020 1:46 PM	Text Document	1 KB
	<i>*</i>	📄 CCEDataProtectTool 🗲	3/5/2020 1:46 PM	Text Document	2 KB
ds	*	ServiceAccountManager	3/5/2020 1:38 PM	Text Document	20 KB