瞭解UCCE 12.5安全增強功能

目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>背景資訊</u> <u>驗證下載的ISO</u> <u>使用SHA-256和金鑰大小2048位的證書</u> <u>SSLUtil工具</u> <u>DiagFwCertMgr命令</u> 資料保護工具

簡介

本檔案介紹整合客服中心企業版(UCCE)12.5新增的最新安全增強功能。

必要條件

- UCCE
- 開放式安全套接字層(SSL)

需求

思科建議您瞭解以下主題:

- UCCE 12.5
- 開啟SSL

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- UCCE 12.5
- •Windows版OpenSSL(64位)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

背景資訊

思科安全控制架構(SCF):合作安全控制框架為構建安全可靠的合作基礎設施提供了設計和實施指南 。這些基礎設施可抵禦眾所周知和新形式的攻擊。Cisco <u>Unified ICM/Contact Center Enterprise參</u> 考安全指南,版本12.5。 作為思科SCF工作的一部分,為UCCE 12.5新增了其他安全增強功能。本文檔概述了這些增強功能。

驗證下載的ISO

為了驗證由思科簽署的已下載ISO並確保其獲得授權,請執行以下步驟:

1.下載並安裝OpenSSL。搜尋軟體「openssl softpedia」。

SOFTPEDIA"	IN WINDOWS	🖛 DRIVERS	CAMES	C HAC	ANDROID APK	🛎 LINUX	IN NEWS & REVIEWS	💛 i	3
Softpetia > Windows > Program	ming > Components l	Ebraries > 0	perSil.		IRCE TRUE, 📥 Data	ver Booster	6 PRO (60% OFF why	en you buy	A
Advertisement									_
🔒 OpenSSL							Search	4	a,
								_	

2.確認路徑(預設情況下已設定,但仍可用於驗證)。 在Windows 10中,轉至「系統屬性」,選擇 「環境變數」。

Edit System Variable		×
Variable name: OPENS	SL_CONF	
Variable value: C:\Ope	nSSL-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驗證所需的檔案

	>	This	PC > Local Disk (C:) > ISO	5 ~	Search ISO	ېر
		^	Name	Date modified	Туре	Size
22			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	R		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.從命令列運行OpenSSL工具。

5. 執行命令

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

6.如果失敗,命令列會顯示錯誤,如下圖所示

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>

使用SHA-256和金鑰大小2048位的證書

日誌會報告識別非投訴證書時的錯誤(即不符合SHA-256和/或keysize 2048位的要求)。

從UCCE的角度來看,有兩個重要證書:

- Cisco ICM診斷框架服務證書
- Cisco ICM SSL憑證

可以在Windows伺服器的Internet資訊服務(IIS)管理器選項中檢視證書。



對於自簽名證書(用於診斷門戶或Web設定),報告的錯誤行為:

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

SSLUtil工具

a.若要重新生成自簽名證書(對於WebSetup/CCEAdmin頁),請使用SSLUtil工具(從位置 C:\icm\bin獲取)。

b.選擇Uninstall刪除當前的「Cisco ICM SSL Certificate」。

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] SSLIS enabled for pin 12-sise-spin 12_scriptmon [Information] [SSLUtil] Comparing input: C:\icm\ssl\cfg\server-iis xml output: C:\i	icm\tomca	it\conf\se	rvero				
[Information] [SSLUtil] Compare() files are the same							
[Information] [SSLUtil] SSL is not enabled for common->setup->jakarta							
<			>				
Clear		Close					

c.接下來選擇「安裝在SSLUtil工具中」,在過程完成之後,請注意現在建立的證書包括SHA-256和 keysize '2048'位。

	💀 Certificate 🛛 🗙
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	Signature algorithm sha256RSA
Cisco ICM Diagnostic Framew aw12 samaira.com	Signature hash algorithm sha256
Cisco ICM SSL Certificate aw12 samaira com	Issuer aw12.samaira.com
cisco icivi sse certificate awiz.samaira.com	📴 Valid from Tuesday, March 26, 2019 2:5
	📴 Valid to Monday, March 21, 2039 2:50
	Subject aw 12. samaira.com
	Public key RSA (2048 Bits)
	Public key parameters 05 00

DiagFwCertMgr命令

若要為Cisco ICM診斷框架服務證書重新生成自簽名證書,請使用命令列「**DiagFwCertMgr**」,如 下圖所示:

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>_

資料保護工具

1. CCEDataProtectTool用於加密和解密Windows登錄檔儲存在其中的敏感資訊。升級到SQL 12.5後,需要使用CCEDataProtectTool重新配置**SQLogin註**冊表中儲存的值。只有管理員、具有管 理許可權的域使用者或本地管理員可以運行此工具。

2.此工具可用於檢視、配置、編輯、刪除SQLogin登錄檔中的加密值儲存。

3.在位置找到工具;

<Install Directory>:\icm\bin\CCEDataProtectTool.exe 4.導航到位置,然後按兩下CCEDataProtectTool.exe。

File Home	Share	View Manage				~ 🕐
← → ▼ ↑	→ Thi	s PC > Local Disk (C:) > icm > bin		✓ 🖑 Search bir	1	Ą
		Name	Date modified	Туре	Size	^
📌 Quick access		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	*	💿 cdbin	4/18/2020 11:50 PM	Windows Batch File	1 KB	

5.若要加密,請按1對DBLookup,請輸入例項名稱。接下來,按2選擇「Edit and Encrypt」

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 4 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 . Decrypt and View Edit and Encrypt Help 4. Exit

6. 導航至登錄檔位置並檢視字串值SQLogin顯示為空白,如下圖所示:

<pre>iKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\pin12\RouterA\Router\CurrentVersion\Configuration\Database</pre>						
Name	Туре	Data				
(Default)	REG_SZ	(value not set)				
R AbandonTimeout	REG DWORD	0x00001388 (5000)				
ab SQLLogin	REG_SZ					
ue inreads	REG_DWORD	0x00000005 (5)				
3 Timeout	REG_DWORD	0x0000015e (350)				
Edit String		x				
Value name:						
SQLLogin						
Value data:						
		OK Cancel				

7.在需要檢查加密值的情況下;在CCEDataProtectTool的命令列中,選擇「Decrypt and View」 (解密和檢視)按1,如下圖所示;



8.在位置可以找到此工具的任何日誌;

<Install Directory>:\temp

Audit logs filename : CCEDataProtectTool_Audit CCEDataProtectTool logs : CCEDataProtectTool

	> This	PC > Local Disk (C:) > Temp >	~ (Search Temp	م
		Name	Date modified	Туре	Size
-55		🖹 CCEDataProtectTool_Audit ←	3/5/2020 1:46 PM	Text Document	1 KB
		📄 CCEDataProtectTool 🗲	3/5/2020 1:46 PM	Text Document	2 KB
ds	R	ServiceAccountManager	3/5/2020 1:38 PM	Text Document	20 KB