Introducción a las mejoras de seguridad de UCCE 12.5

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Antecedentes Verificación de ISO descargado Utilizar certificados con bits SHA-256 y tamaño de clave 2048 Herramienta SSLUtil Comando DiagFwCertMgr Herramienta de protección de datos

Introducción

Este documento describe las últimas mejoras de seguridad añadidas con Unified Contact Center Enterprise (UCCE) 12.5.

Prerequisites

- UCCE
- Capa de sockets seguros abierta (SSL)

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- UCCE 12.5
- Open SSL

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- UCCE 12.5
- OpenSSL (64 bits) para Windows

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Marco de control de seguridad de Cisco (SCF): El marco de control de seguridad de colaboración proporciona las directrices de diseño e implementación para crear infraestructuras de colaboración seguras y fiables. Estas infraestructuras son resistentes a las formas de ataque conocidas y nuevas. <u>Guía</u> de <u>seguridad de</u> referencia <u>para Cisco Unified ICM/Contact Center</u> <u>Enterprise, versión 12.5</u>.

Como parte del esfuerzo de SCF de Cisco, se añaden mejoras de seguridad adicionales para UCCE 12.5. Este documento describe estas mejoras.

Verificación de ISO descargado

Para validar la ISO descargada firmada por Cisco y asegurarse de que está autorizada, los pasos son:

1. Descargue e instale OpenSSL. Busque software "openssl softpedia".

$\leftarrow \rightarrow$	X # softpedia.com/get/?rogn	amming/Components-Li	braries/OpenSSLa	icrol					11	r.
	SOFTPEDIA"	🛤 WINDOWS 📼	idanes 🕳 Gr	MES 🔹 NAC	ANDROID APK	🛎 LINUX	B NEWS & REVIEWS	: + i	1	
	Solpedia > Windows > Prop.	anning > Components & L	braies > OperSSL		IRCE TRUAL 🔺 Data	ver Booster	6 PRO (60% OFF with	en you buy)		
	Advortisiement									
	🔒 OpenSSL						Search	Q	L	
	O DOWINLOAD NOW	89,765 downloads - Up	dated December 22.	2029 - FREDAN	1 O		****	405 24	8	
				1						

2. Confirme la ruta (se establece de forma predeterminada , pero sigue siendo buena para verificar). En Windows 10, vaya a Propiedades del sistema, seleccione Variables de entorno.

Edit System Variable	-	×
Variable name: OP	ENSSL_CONF	
Variable value:	OpenSSL-Win64\bin\openssl.cfg	
Browse Directory	Browse File	OK Cancel
JAVA_HOME JAVA_OPTS NUMBER_OF_PROCESSO	C:\Program Files (x86)\Java\jre1.8.0_221 -Dbundle.provider.className=com.cisco.c RS 6	ccbu.cce.cceadmin.i18n
OPENSSL_CONF OS	C:\OpenSSL-Win64\bin\openssl.cfg Windows_NT	

3. Archivos necesarios para la verificación ISO

	>	This	PC > Local Disk (C:) > ISO	~ 2	5 Search ISO	۶
		^	Name	Date modified	Туре	Size
55			CCEInst1251	2/24/2020 2:31 PM	WinRAR archive	1,129,294 KB
	я		CCEInst1251.iso.md5	2/24/2020 2:27 PM	MD5 File	1 KB
ls	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. Ejecute la herramienta OpenSSL desde la línea de comandos.



5. Ejecute el comando

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

6. En caso de error, la línea de comandos muestra el error como se muestra en la imagen

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>

Utilizar certificados con bits SHA-256 y tamaño de clave 2048

Los registros informan de un error en el caso de identificar certificados que no son de queja (es decir, no cumplen con el requisito SHA-256 y/o tamaño de clave 2048 bits).

Hay dos certificados importantes desde la perspectiva de UCCE:

- Certificado de servicio de Cisco ICM Diagnostic Framework
- Certificado Cisco ICM SSL

Los certificados se pueden revisar en la opción Administrador de Internet Information Services (IIS) del servidor de Windows.



Para los certificados autofirmados (ya sea para Diagnose Portico o Web Setup), la línea de error informada es:

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

Herramienta SSLUtil

a. Para regenerar certificados autofirmados (para la página WebSetup/CCEAdmin), utilice la herramienta SSLUtil (desde la ubicación C:\icm\bin).

b. Seleccione Uninstall (Desinstalar) para eliminar el "Cisco ICM SSL Certificate" actual.

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] adding instance pin12 with app count of 1							
[Information] [SSLUtil] SSL is enabled for pin12->ise->pin12_scriptmon		00					
[Information] [SSLUtil] Comparing input: C: \cm \ssi \crg \server+is \xmi output: C: \ [Information] [SSLUtil] Compare() files are the same	icm tomca	it \cont\se	rvero				
[Information] [SSLUtil] SSL is not enabled for common->setup->jakarta							
<			>				
Clear	_	Close					

c. A continuación, seleccione Install in SSLUtil tool y, una vez que el proceso haya finalizado, observe que el certificado creado ahora incluye los bits SHA-256 y el tamaño de clave '2048'.

	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 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 Signature hash algorithm sha256 Super aw12.samaira.com Valid from Tuesday, March 26, 2019 2:5 Valid to Monday, March 21, 2039 2:50
	Public key parameters 05 00

Comando DiagFwCertMgr

Para regenerar un certificado autofirmado para el certificado de servicio de Cisco ICM Diagnostic

Framework, utilice la línea de comandos "DiagFwCertMgr", como se muestra en la imagen:

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>_

Herramienta de protección de datos

1. CCEDataProtectTool se utiliza para cifrar y descifrar la información confidencial que almacena el Registro de Windows en él. Después de actualizar a SQL 12.5, el almacén de valores en el registro **SQLLogin** debe reconfigurarse con CCEDataProtectTool. Sólo el administrador, el usuario de dominio con derechos administrativos o un administrador local pueden ejecutar esta herramienta.

2. Esta herramienta se puede utilizar para ver, configurar, editar, eliminar el almacén de valores cifrado en el registro **SQLLogin**.

3. La herramienta se encuentra en la ubicación;

<Install Directory>:\icm\bin\CCEDataProtectTool.exe

4. Desplácese hasta la ubicación y haga doble clic en CCEDataProtectTool.exe.

File Home	Share	View Manage				~ 🕐
← → → ↑) > Thi	s PC → Local Disk (C:) → icm → bin		✓ ♂ Search bir	n	Q
		Name	Date modified	Туре	Size	^
📌 Quick access		CCEDataProtectTool	7/2020 3:37 PM	Application	54 KB	
👆 Downloads	*	الله دcisCommon الله الم	12/19/2019 7:47 AN	1 Executable Jar File	1,403 KB	
📃 Desktop	*	🗋 cdbin.ba_	12/19/2019 7:48 AN	1 BA_ File	1 KB	
Documents	*	💿 cdbin	4/18/2020 11:50 PM	1 Windows Batch File	1 KB	

5. Para cifrar , presione 1 para DBLookup, ingrese Instance Name . A continuación, pulse 2 para seleccionar "Editar y cifrar"

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 ← 2. Rekey 3. 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. Navegue hasta la ubicación del Registro y revise el aspecto en blanco del valor de cadena SQLLogin , como se muestra en la imagen :

<pre>HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\pin12\RouterA\Router\CurrentVersion\Configuration\Database</pre>							
Name	Туре	Data					
ab (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		x					
Value name:							
Value data:							
		OK Cancel					

7. En caso de necesidad de revisar el valor cifrado; mientras que la línea de comandos de CCEDataProtectTool, seleccione pulsar 1 para "Descifrar y ver", como se muestra en la imagen;



8. Los registros de esta herramienta se pueden encontrar en la ubicación;

<Install Directory>:\temp

Audit logs filename : CCEDataProtectTool_Audit CCEDataProtectTool logs : CCEDataProtectTool

	> Th	is PC > Local Disk (C:) > Temp >	~	ප Search Temp	م ر
		Name	Date modified	Туре	Size
255		🖹 CCEDataProtectTool_Audit ←	3/5/2020 1:46 PM	Text Document	1 KB
	*	🖹 CCEDataProtectTool 🗲	3/5/2020 1:46 PM	Text Document	2 KB
ds		ServiceAccountManager	3/5/2020 1:38 PM	Text Document	20 KB