Compreenda as melhorias de segurança do UCCE 12.5

Contents

Introduction Prerequisites Requirements Componentes Utilizados Informações de Apoio Verificação da ISO baixada Usar certificados com SHA-256 e tamanho de chave 2048 bits Ferramenta SSLUtil Comando DiagFwCertMgr Ferramenta de proteção de dados

Introduction

Este documento descreve os aprimoramentos de segurança mais recentes adicionados ao Unified Contact Center Enterprise (UCCE) 12.5.

Prerequisites

- UCCE
- Open Secure Sockets Layer (SSL)

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- UCCE 12.5
- SSL aberto

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Cisco Security Control Framework (SCF): A estrutura de controle de segurança de colaboração fornece as diretrizes de projeto e implementação para a criação de uma infraestrutura de colaboração segura e confiável. Essas infraestruturas são resilientes a formas conhecidas e novas de ataques. <u>Guia de Segurança de</u> Referência <u>do Cisco Unified ICM/Contact Center</u> <u>Enterprise, Versão 12.5</u>.

Como parte do esforço de SCF da Cisco, melhorias de segurança adicionais são adicionadas para UCCE 12.5. Este documento descreve esses aprimoramentos.

Verificação da ISO baixada

Para validar o ISO baixado assinado pela Cisco e garantir que ele seja autorizado, as etapas são:

1. Baixe e instale o OpenSSL. Procure por software "openssl softpedia".

→ × i softpedi	a.com/get/Programs	ning/Components-	Libraries/Ope	erSSLahtml					
SOFTP	EDIA"	I WINDOWS	🖛 DANEIS	📾 GAMES	е нис	ANDROID APK	â LINUX	IN NEWS & REVIEWS	
■ SiOpelia	Windows > Program	ning > Components I	Ubraries > 0	per SSL		IRCE TRUAL 📥 Dat	ver Booster	6 FRO (60% OFF whe	m you buy!
Advertisement									
🔒 Oper	nSSL							Search	Q,
O DOW	NLOAD NOW	89,705 downloads - I	Updated Decen	ber 22, 2029	TREAM	0		****	405 24 8

2. Confirme o caminho (definido por padrão, mas ainda é bom verificar). No Windows 10, vá para Propriedades do sistema, selecione Variáveis de ambiente.

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

3. Arquivos necessários para a verificação 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	Å		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. Execute a ferramenta OpenSSL a partir da linha de comando.



5. Executar o comando

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

6. Em caso de falha, a linha de comando mostra um erro como mostrado na imagem

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>

Usar certificados com SHA-256 e tamanho de chave 2048 bits

Os registros reportam um erro no caso de identificação de certificados não reclamantes (isto é, não atendem ao requisito SHA-256 e/ou keysize 2048 bits).

Há dois certificados importantes do ponto de vista do UCCE:

- certificado de serviço do Cisco ICM Diagnostic Framework
- Certificado SSL do Cisco ICM

Os certificados podem ser revisados na opção Gerenciador dos Serviços de Informações da Internet (IIS) do Windows Server.



Para certificados autoassinados (para Diagnose Portico ou Configuração da Web), a linha de erro reportada é:

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

Ferramenta SSLUtil

a. Para gerar novamente certificados autoassinados (para a página WebSetup/CCEAdmin), use a ferramenta SSLUtil (na localização C:\icm\bin).

b. Selecione Desinstalar para excluir o "Certificado SSL do Cisco ICM" atual.

👌 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[U]: pin 12 [Information] [SSLUtil] adding instance pin 12 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	icm\tomca	t\conf\se	rvero				
[Information] [SSLUtil] Compare() files are the same [Information] [SSLUtil] SSL is not enabled for common->setup->iakarta							
<			>				
Clear		Close					

c. Em seguida, selecione Instalar na ferramenta SSLUtil e, depois que o processo for concluído, observe que o certificado criado agora inclui os bits SHA-256 e keysize '2048'.

	💀 Certificate 🛛 🗙
Server Certificates	General Details Certification Path
Use this feature to request and manage certificates that the Web ser	N 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 Issuer aw12.samaira.com Valid from Tuesday, March 26, 2019 2:5 Valid to Monday, March 21, 2039 2:50 Subject aw12.samaira.com
	Public key RSA (2048 Bits)

Comando DiagFwCertMgr

Para regenerar um certificado autoassinado para o certificado de serviço do Cisco ICM Diagnostic

Framework, use a linha de comando "DiagFwCertMgr", como mostrado na imagem:

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>_

Ferramenta de proteção de dados

1. CCEDataProtectTool é usado para criptografar e descriptografar informações confidenciais que o registro do Windows armazena nele. Após a atualização para SQL 12.5, o armazenamento de valores no registro **SQLLogin** precisa ser reconfigurado com CCEDataProtectTool. Somente administrador, usuário de domínio com direitos administrativos ou um administrador local pode executar essa ferramenta.

2. Esta ferramenta pode ser usada para visualizar, configurar, editar, remover armazenamento de valores criptografados no registro **SQLLogin**.

3. A ferramenta está no local;

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

4. Navegue até o local e clique duas vezes em 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 criptografar , pressione 1 para DBLookup, insira Instance Name (Nome de instância). Em seguida, pressione 2 para selecionar "Edit and Encrypt" (Editar e criptografar)

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 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 3. Help 4. Exit

6. Navegue até o local do registro e reveja o SQLLogin do valor da string parece em branco, como mostrado na imagem :

<pre>inc.\ICM\pin12\RouterA\Router\CurrentVersion\Configuration\Database</pre>						
Name	Туре	Data				
(Default)	REG_SZ	(value not set)				
30 AbandonTimeout	REG DWORD	0x00001388 (5000)				
ab) SQLLogin	REG_SZ					
ue inreads	REG_DWORD	0x0000005 (5)				
🐯 Timeout	REG_DWORD	0x0000015e (350)				
Edit String		×				
Value name:						
SQLLogin						
Value data:						
		OK Cancel				

7. Em caso de necessidade de rever o valor encriptado; enquanto linha de comando do CCEDataProtectTool, selecione pressionar 1 para "Descriptografar e visualizar", como mostrado na imagem;

INTER LOCAL MACHINEL CODERADEL C.



8. Os registros desta ferramenta podem ser encontrados no local;

<Install Directory>:\temp

Audit logs filename : CCEDataProtectTool_Audit CCEDataProtectTool logs : CCEDataProtectTool

	> Th	is PC → Local Disk (C:) → Temp →	~	Ö	Search Temp	م ر
		Name	Date modified	Ту	pe	Size
255		🖹 CCEDataProtectTool_Audit 🗲	3/5/2020 1:46 PM	Те	at Document	1 KB
	*	🖹 CCEDataProtectTool 🗲	3/5/2020 1:46 PM	Te	of Document	2 KB
ds		ServiceAccountManager	3/5/2020 1:38 PM	Te	at Document	20 KB