

Identity Services Engine:Mudhraルートおよび中間認証局に対する緊急不信

内容

目的

以下は、Mudhraルートおよび中間認証局を緊急に信頼しないIdentity Services Engine(ISE)およびISE PIC (パッシブIDコネクタ) に関するガイダンスです。Identity Service Engine(ISE)の設定には、影響を受けるMudhraルートおよび中間認証局がデフォルトでは信頼ストアに含まれていませんが、ISEの設定を見直して、インストール後の設定で使用されていないことを確認する必要があります。

免責事項

この記事は、影響を受ける認証局の存在に関するISE設定のレビューを支援することを目的としています。Identity Services Engine全体は現在も調査中で、今後さらに設定やソフトウェアの更新が必要になる可能性があります。この記事は、
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-emudhra-info-ScS22A1r>にあるセキュリティアドバイザリとともに更新されます。

システム証明書

Administration -> System -> Certificates -> System Certificatesの順に表示し、ノード1x1に割り当てられている各証明書を選択して、viewを選択します。[1]



Certificate Hierarchy

Certificate Services Root CA - zer0k-ise1

Certificate Services Node CA - zer0k-ise1

Certificate Services Endpoint Sub CA - zer0k-ise1

zer0k-ise1.zer0k.org



zer0k-ise1.zer0k.org

Issued By : Certificate Services Endpoint Sub CA - zer0k-ise1

Expires : Mon, 4 Aug 2031 10:52:08 EDT

Certificate status is good

Details

Issued To

Common Name (CN) zer0k-ise1.zer0k.org

影響を受けるCAまたは発行側の証明書が証明書階層にないことを確認します。これらの証明書を使用している場合は、そのサービスを新しい認証局に移行する手順を開始します。

信頼できる証明書

Administration -> System -> Certificates -> Trusted Certificatesの順に選択し、インストールされたルート証明書と中間証明書のリストを確認します。Trustedリストに影響を受けるCAが1つ以上見つかった場合は、「Trusted For」列に注目し、各タイプ[2]に対して次のアクションを実行します。

☐	Friendly Name	Trusted For	Serial Number	Issued To	Issued By	Valid From
		Endpoints				
☐	Cisco Root CA 2048	Endpoints Infrastructure	5F F8 7B 28 2...	Cisco Root CA 2048	Cisco Root CA 2048	Fri, 14 May 2004
☐	Cisco Root CA 2099	Cisco Services	01 9A 33 58 7...	Cisco Root CA 2099	Cisco Root CA 2099	Tue, 9 Aug 2016
☐	Cisco Root CA M1	Infrastructure Cisco Services Endpoints AdminAuth NativeIPSec	2E D2 0E 73 4...	Cisco Root CA M1	Cisco Root CA M1	Tue, 18 Nov 20...

- ・ シスコサービス：シスコはeMudhraをサービスに使用しません。これが唯一のエントリである場合、証明書を削除できます。
- ・ インフラストラクチャ：エンドポイントまたはAdminAuthロール、あるいはその両方が不要であることを確認し、CAまたは発行者からの証明書がシステム証明書の下で使用されていないことを確認します。
- ・ Endpoints：エンドポイントが侵害されたチェーンを必要とするかどうかを確認します。エンドポイントがCAまたは発行者を使用しているかどうかわからない場合は、「クライアント認証およびSyslogに対する信頼」オプションを無効にし、クライアント認証の失敗に関するライブログとレポートを監視します。
- ・ AdminAuth：新しい証明書の発行中にクイックオプションの管理者認証をパスワードベースのログインに戻せるように、管理者に新しい証明書を発行します。
- ・ NativeIPSec:Native IPsec機能を使用している場合、IPSecクライアントを新しいCAに移行します

その他のサービス

影響を受ける信頼できる証明書を削除しても、システムの機能に影響が及ばないように、次のサービス設定を確認する必要があります。これらのサービスを使用している場合は、信頼できる証明書を削除する前に、新しい証明書を使用するようにサービスを再設定する必要があります。

[LDAP]

Administration -> Identity Management -> External Identity Sources -> LDAPの順に表示します。各LDAPエントリの下でConnectionタブをクリックします。Secure Authenticationが有効になっている場合は、「LDAP Server Root CA」および「Issuer CA of ISE Certificates」設定のチェーンを確認します。[3]

LDAP Server Root CA	VeriSign Class 3 Public Pri... 	LDAP Server Root CA	VeriSign Class 3 Public Pri... 
Issuer CA of ISE Certificates	DigiCert Global Root CA  	Issuer CA of ISE Certificates	Select if required (optional) 

SYSLOG

Administration -> System -> Logging -> Remote Logging Targetsの順に選択し、設定されているSecure SYSLOG Serverで、設定されている信頼されたルート証明書を確認します。影響を受けるCA証明書のいずれかが使用されている場合、SYSLOGサーバのチェーンを確認し、必要に応じて新しいルートを再発行して信頼します。[4]

Select CA Certificate

Cisco Root CA M1



Note: The CA certificates should be imported into the Certificate Store, enabled, and trusted for client authentication prior to configuring Secure Syslog. Ensure that a local certificate signed by the selected CA exists on the primary and secondary nodes.

If a local certificate signed by the selected CA does not exist, the self-signed local certificate will be used.

Ignore Server Certificate validation

☐

RADIUSのDTLS

オプションで、[Administration] -> [Network Resources] -> [Network Devices]の各ネットワークデバイスの下で、[Issuer CA of ISE Certificates for CoA]を設定できます。この設定は、DTLS用に設定されたネットワークデバイスにCoAを発行するためにISEが使用するクライアント証明書の選択にのみ使用されます。証明書はノードのISEのSystem Certificatesページに表示されるため、この設定は、いずれかのMudhra証明書からの証明書の発行がISEノードに対して発行された場合にのみ、各設定ネットワークデバイスについて確認する必要があります。

[1] [ISEでの証明書管理](#)

[2] [ISEの信頼できる証明書の設定](#)

[3] [ISEセキュアLDAP設定](#)

[4] [セキュアなsyslogリモートロギングターゲットの設定](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。