

Identity Services Engine - Emergency Distrust of eMudhra Root and Intermediate Certificate Authorities

Contents

Purpose

Below is the guidance on Identity Services Engine and ISE PIC (Passive Identity Connector) for the emergency distrust of eMudhra Root and Intermediate Certificate Authorities. Identity Service Engine configuration does not include the impacted eMudhra Root and Intermediate Certificate Authorities by default in the Trusted Store, but the ISE configuration should be reviewed to ensure they are not in use via post install configuration.

DISCLAIMER

This article is only meant to assist in reviewing the ISE configuration for presence of the impacted certificate authorities. Identity Services Engine as a whole is still being investigated and may require further configuration or software updates in the future. This article will be updated along with the Security Advisory located at <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-emudhra-info-ScS22A1r>.

System Certificates

Browse to Administration -> System -> Certificates -> System Certificates, select each certificate assigned to the nodes 1 by 1 and select view. [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

Ensure that the impacted CA or Issuing certificates are not in the Certificate Hierarchy. If they are in use, begin taking steps to migrate that service to a new certificate authority.

Trusted Certificates

Browse to Administration -> System -> Certificates -> Trusted Certificates and review the list of installed root and intermediate certificates. If you do find one or more of the impacted CAs in the Trusted list, note the "Trusted For" column and take the following action for each type [2]:

☐	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...

- Cisco Services - Cisco does not use eMudhra for any service, if this is the only entry the certificate can be deleted.
- Infrastructure - Verify that the Endpoints and/or AdminAuth role is not required, verify that no certificate from the CA or Issuers are being used under System Certificates
- Endpoints - Verify if endpoints are authenticating requiring the compromised chain, if unsure if endpoints are using the CA or Issuers, disable the "Trust for client authentication and Syslog" option and monitor live logs and reports for client authentication failures.
- AdminAuth - Issue new certificates to your administrators, as a quick option Admin Authentication can be moved back to password based login while new certificates are being issued.
- NativeIPSec - If using the Native IPSec feature, migrate the IPSec clients to a new CA

Other Services

The following service configurations should be reviewed to ensure deleting any impacted trusted certificates will not impact the function of the system. If they are in use by these services, the services should be reconfigured to use new certificates before the trusted certificates are deleted.

LDAP

Browse to Administration -> Identity Management -> External Identity Sources -> LDAP. Under each LDAP entry, click on the Connection tab, if Secure Authentication is enabled verify the chain for "LDAP Server Root CA" and "Issuer CA of ISE Certificates" settings. [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

Browse to Administration -> System -> Logging -> Remote Logging Targets, view each configured Secure SYSLOG Server for the configured Trusted Root certificate, if one of the impacted CA certificates is in use, verify the chain on the SYSLOG server and re-issue and trust a new root if needed. [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 DTLS

It is possible to optionally set the "Issuer CA of ISE Certificates for CoA" under each each Network Device under Administration -> Network Resources -> Network Devices. This setting is only used to select the client certificate that ISE will use to issue a CoA to a network device configured for DTLS. The certificate will displayed on the System Certificates page in ISE for the node so this setting will only need to be verified for each configure network device if a certificate issue from one of the eMudhra certificates is issued to an ISE node.

[1] [Certificate Management in ISE](#)

[2] [ISE Trusted Certificate Settings](#)

[3] [ISE Secure LDAP Configuration](#)

[4] [Configure Secure Syslog Remote Logging Target](#)