

ISE(Identity Services Engine) - Mudhra 루트 및 중간 인증 기관에 대한 긴급 불신

목차

목적

아래는 Mudhra 루트 및 중간 인증 기관에 대한 긴급 불신을 위한 Identity Services Engine 및 ISE PIC(Passive Identity Connector)에 대한 안내입니다. Identity Service Engine 컨피그레이션에는 기본적으로 신뢰할 수 있는 저장소에 영향을 받는 Mudhra 루트 및 중간 인증 기관이 포함되어 있지 않지만, 설치 후 컨피그레이션을 통해 ISE 컨피그레이션이 사용되지 않는지 확인해야 합니다.

면책조항

이 문서는 영향을 받는 인증 기관이 있는지 ISE 컨피그레이션을 검토하는 데만 도움이 됩니다. ISE(Identity Services Engine) 전체가 아직 조사 중이며 향후 추가 컨피그레이션 또는 소프트웨어 업데이트가 필요할 수 있습니다. 이 문서는 <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-emudhra-info-ScS22A1r>에 있는 Security Advisory와 함께 [업데이트됩니다](#).

시스템 인증서

Administration(관리) -> System(시스템) -> Certificates(인증서) -> System Certificates(시스템 인증서)로 이동하여 노드에 할당된 각 인증서를 1씩 선택하고 view(보기)를 선택합니다. [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

영향을 받는 CA 또는 발급 인증서가 인증서 계층 구조에 없는지 확인합니다. 사용 중인 경우 해당 서비스를 새 인증 기관으로 마이그레이션하기 위한 단계를 시작합니다.

신뢰할 수 있는 인증서

Administration(관리) -> System(시스템) -> Certificates(인증서) -> Trusted Certificates(신뢰할 수 있는 인증서)로 이동하고 설치된 루트 및 중간 인증서 목록을 검토합니다. Trusted(신뢰할 수 있는) 목록에서 하나 이상의 영향을 받는 CA를 찾은 경우 "Trusted For(신뢰할 수 있는 대상)" 열을 확인하고 각 유형 [2]에 대해 다음 작업을 수행합니다.

☐	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(시스코 서비스) - 인증서가 삭제될 수 있는 유일한 항목인 경우 Cisco는 모든 서비스에 대해 eMudhra를 사용하지 않습니다.
- 인프라 - 엔드포인트 및/또는 AdminAuth 역할이 필요하지 않은지, CA 또는 발급자의 인증서가 시스템 인증서에서 사용되고 있지 않은지 확인합니다.
- Endpoints(엔드포인트) - 엔드포인트가 손상된 체인을 필요로 하여 인증되고 있는지 확인하고, 엔드포인트가 CA 또는 발급자를 사용하고 있는지 확실하지 않은 경우 "Trust for client authentication and Syslog" 옵션을 비활성화하고 클라이언트 인증 실패에 대한 라이브 로그 및 보고서를 모니터링합니다.
- AdminAuth - 관리자에게 새 인증서를 발급합니다. 새 인증서가 발급되는 동안 관리자 인증을 비밀번호 기반 로그인으로 다시 이동할 수 있는 빠른 옵션입니다.
- NativeIPSec - Native IPsec 기능을 사용하는 경우 IPsec 클라이언트를 새 CA로 마이그레이션합니다

기타 서비스

영향을 받는 신뢰할 수 있는 인증서를 삭제해도 시스템 기능에 영향을 주지 않도록 다음 서비스 구성을 검토해야 합니다. 이러한 서비스를 사용 중인 경우 신뢰할 수 있는 인증서를 삭제하기 전에 새 인증서를 사용하도록 서비스를 다시 구성해야 합니다.

LDAP

Administration(관리) -> Identity Management(ID 관리) -> External Identity Sources(외부 ID 소스) -> LDAP로 이동합니다. 각 LDAP 항목 아래에서 Connection(연결) 탭을 클릭합니다. 보안 인증이 활성화된 경우 "LDAP Server Root CA(LDAP 서버 루트 CA)" 및 "Issuer CA of ISE Certificates(ISE 인증서의 발급자 CA)" 설정의 체인을 확인합니다. [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(관리) -> System(시스템) -> Logging(로깅) -> Remote Logging Targets(원격 로깅 대상)로 이동하여 구성된 각 Secure SYSLOG Server(보안 SYSLOG 서버)에서 구성된 트러스트된 루트 인증서를 확인하고, 영향을 받은 CA 인증서 중 하나가 사용 중인 경우 SYSLOG 서버의 체인을 확인하고, 필요한 경우 새 루트를 다시 발급하고 트러스트합니다. [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

Administration(관리) -> Network Resources(네트워크 리소스) -> Network Devices(네트워크 디바이스) 아래에서 각 네트워크 디바이스 아래에 "CoA용 ISE 인증서의 발급자 CA"를 선택적으로 설정할 수 있습니다. 이 설정은 ISE가 DTLS에 대해 구성된 네트워크 디바이스에 CoA를 발급하는 데 사용할 클라이언트 인증서를 선택하는 데만 사용됩니다. 인증서는 노드에 대한 ISE의 시스템 인증서 페이지에 표시되므로 이 설정은 eMudhra 인증서 중 하나에서 발급된 인증서가 ISE 노드에 발급된 경우 각 네트워크 디바이스를 구성하는 경우에만 확인하면 됩니다.

[1] [ISE의 인증서 관리](#)

[2] [ISE 신뢰할 수 있는 인증서 설정](#)

[3] [ISE 보안 LDAP 컨피그레이션](#)

[4] [보안 Syslog 원격 로깅 대상 구성](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.