Troubleshoot Telepresence SUDI Certificate Chain Security Scan Findings

Contents

Issue

Security vulnerability scans are flagging SSL/TLS certificate-related findings on Cisco Telepresence video codec endpoints, specifically reporting an untrusted certificate chain on TCP ports 4053, 4060, and 4062. The vulnerability scanner identifies the codec presents a CS-Room certificate issued by ACT2 SUDI CA (Organization: Cisco) with the certificate chain terminating at Cisco Root CA 2048. The security scanning system reports this as an untrusted certificate chain that does not meet organizational security requirements.

The specific findings reported by security scans include:

- Self-signed certificate detection
- Untrusted certificate chain
- Weak hashing algorithm concerns
- Certificate expiry warnings

Environment

- Cisco Telepresence video codec endpoints
- Webex Desk Series devices with on-premises registration
- Endpoints with ACT2 SUDI (Secure Unique Device Identifier) chips
- Security vulnerability scanning infrastructure flagging certificate chain issues
- TCP ports 4053, 4060, and 4062 presenting SUDI certificates

Resolution

The SUDI certificates on Cisco Telepresence endpoints are embedded, immutable certificates that cannot be modified, regenerated, or deleted in a supported manner. These certificates are part of Cisco's Trustworthy Technologies implementation and serve specific security functions.

Understanding SUDI Certificate Behavior

The certificate behavior varies by port and system configuration:

- **Port 4053 (Pairing Service):** Uses SUDI certificates when the system has an ACT2 chip. Custom certificates are only used on systems without an ACT2 chip (older endpoints).
- **Port 4047:** Uses customer-chosen certificates for communication between touch panels and codecs.

Certificate Location and Details

The SUDI certificates are located in the device's certificate store:

```
device:~] $ cd /etc/cacerts_sudi
device:/etc/cacerts_sudi] $ ls
0763c37d.0                9426d327.0                mic-cbasrcarsa4k2099.pem
29cf4e89.0                a094437b.0                mic-cmca.pem
36087b08.0                b35c8d6c.0                mic-cmca2.pem
417aa245.0                cmca2.pem                 mic-cmca3.pem
771a09b9.0                crca2048.pem              mic-cmca4.pem
89087fe6.0                crca2099.pem              mic-crcam2.pem
90359431.0                mic-cbarc2099.pem         mic-harsa-ca.pem
```

The ACT2 SUDI CA certificate details:

```
CN = ACT2 SUDI CA
O = Cisco
Valid From: Thursday, June 30, 2011 11:26:57 PM
Valid To: Tuesday, May 15, 2029 1:55:42 AM
```

Recommended Actions

Step 1: Review the SUDI certificate purpose and security implementation

The SUDI certificate is not self-signed but is signed by Cisco Manufacturing CA. It serves as an immutable identity credential that:

- Maintains product identifier and serial number
- Provides unchangeable identity for configuration, security, auditing, and management
- Is cryptographically bound to the Trust Anchor module chip
- Makes cloning or spoofing virtually impossible

Step 2: Work with the security team to exclude SUDI certificate findings

Since the SUDI certificates cannot be modified and serve legitimate security functions, the recommended approach is to:

- Configure security scanning tools to exclude the SUDI certificate chain findings for the affected services
- Document the business justification for the exception based on Cisco's Trustworthy Technologies implementation
- Focus security scanning on customer-configurable certificates on other ports if needed

Step 3: Certificate updates through software upgrades

Certificate updates in the trust store occur automatically when the system is upgraded to newer software versions. This ensures certificate validity is maintained over time.

Important Limitations

These limitations apply to SUDI certificates:

- Cannot be modified, regenerated, or deleted
- Automatic regeneration occurs if certificates are deleted and the device restarts
- No supported method exists to assign configurable certificates to these backend services
- Certificate replacement is not possible due to the immutable nature of the Trust Anchor implementation

Cause

The security scan findings are triggered by the presence of Cisco's SUDI (Secure Unique Device Identifier) certificates, which are embedded manufacturing certificates that chain to Cisco Root CA 2048. These certificates are part of Cisco's Trustworthy Technologies implementation and are designed to be immutable for security purposes. The certificates are not recognized as trusted by organizational security scanning tools because they terminate at Cisco's root certificate authority rather than an organization-specific CA. This is expected behavior for SUDI-enabled devices and represents a design feature rather than a security vulnerability.

Related Content

- Cisco Trustworthy Technologies Datasheet
- Cisco Technical Support & Downloads