

Fehlerbehebung bei PKCS#12-Dateiinstallationsfehlern mit nicht FIPS-konformen PBE-Algorithmen

Inhalt

[Einleitung](#)

[Hintergrundinformationen](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Problem](#)

[Lösung](#)

[Verifizierung](#)

Einleitung

In diesem Dokument wird die Fehlerbehebung bei einer fehlgeschlagenen Installation einer PKCS#12-Datei (Public Key Cryptography Standards) mit FIPS-kompatiblen (nicht-Federal Information Processing Standard) PBE-Algorithmen (Password-Based Encryption) über Cisco FirePOWER Management Center (FMC) beschrieben. Es erläutert ein Verfahren, um es zu identifizieren und ein neues kompatibles Paket mit OpenSSL zu erstellen.

Hintergrundinformationen

Cisco Firepower Threat Defense (FTD) unterstützt die Einhaltung von FIPS 140, wenn Sie den Common Criteria (CC)- oder den Unified Capabilities Approved Products List (UCAP)-Modus auf einem verwalteten Gerät aktivieren. Diese Konfiguration ist Teil einer Richtlinie für die FMC-Plattformeinstellungen. Nach dem Anwenden erscheint der Befehl `fips enable` in der Ausgabe von `show running-config` von FTD.

PKCS#12 definiert ein Dateiformat zum Bündeln eines privaten Schlüssels und des entsprechenden Identitätszertifikats. Es besteht die Möglichkeit, ein beliebiges Stamm- oder Zwischenzertifikat einzuschließen, das ebenfalls zur Validierungskette gehört. PBE-Algorithmen schützen die Zertifikate und privaten Schlüsselbereiche der PKCS#12-Datei. Durch die Kombination des Nachrichtenauthentifizierungsschemas (MD2/MD5/SHA1) und des Verschlüsselungsschemas (RC2/RC4/DES) gibt es mehrere PBE-Algorithmen, aber der einzige FIPS-kompatible ist PBE-SHA1-3DES.

 Anmerkung: Weitere Informationen zu FIPS in Cisco Produkten finden Sie unter [FIPS 140](#).

 Anmerkung: Weitere Informationen zu den Sicherheitszertifizierungsstandards für FTD und FMC finden Sie im Kapitel Security Certifications Compliance des [FMC Configuration Guide](#).

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Public Key Infrastructure (PKI)
- OpenSSL

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- FMCv - 6.5.0.4 (Build 57)
- FTDv - 6.5.0 (Build 115)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

 Anmerkung: Der in diesem Dokument beschriebene Ansatz kann auf jeder anderen Plattform mit einem ähnlichen Problem implementiert werden, z. B. einer Cisco Adaptive Security Appliance (ASA), da das Problem bei einem nicht FIPS-konformen Zertifikat liegt.

 Anmerkung: In diesem Dokument wird nicht auf die Bedingung eingegangen, dass die PKCS#12-Komponenten selbst nicht mit anderen Gründen kompatibel sind, wie der Schlüssellänge Rivest, Shamir, Adleman (RSA) oder dem Signaturalgorithmus, der zum Signieren des Identitätszertifikats verwendet wird. In solchen Fällen müssen Zertifikate erneut ausgestellt werden, um FIPS-konform zu sein.

Problem

Wenn der FIPS-Modus in FTD aktiviert ist, schlägt die Zertifikatinstallation möglicherweise fehl, wenn die PBE-Algorithmen, die zum Schutz der PKCS#12-Datei verwendet werden, nicht FIPS-kompatibel sind.

The screenshot shows the Cisco Firepower Management Center (FMC) web interface. The top navigation bar includes tabs for Overview, Analysis, Policies, **Devices**, Objects, AMP, and Intelligence. Below this, there are sub-tabs for Device Management, NAT, VPN, QoS, Platform Settings, FlexConfig, and **Certificates**. The main content area displays a table of certificates:

Name	Domain	Enrollment Type	Status
FTDv_B			
selfsigned_cert	Global	Self-Signed	CA ID
FTD.driverap.com	Global	Manual	CA ID
FTDv_C			
FTDv_C_cert	Global	PKCS12 file	Failed

At the bottom of the interface, there is a status bar showing the last login time and a 'How To' button. An 'Activate Windows' watermark is visible in the bottom right corner.

Anmerkung: Eine schrittweise Anleitung zur Installation einer PKCS#12-Datei mit dem FMC finden Sie im Abschnitt PKCS12 Enrollment (Anmeldung für PKCS12) der [Zertifikatsinstallation und -verlängerung auf dem von FMC verwalteten FTD](#).

Wenn die Zertifikatsinstallation aus diesem Grund fehlschlägt, wird der folgende Fehler vom PKI-Debugging ausgegeben:

```
<#root>
```

```
firepower#
```

```
debug crypto ca 14
```

```
firepower#
```

```
show debug
```

```
debug crypto ca enabled at level 14
```

```
Conditional debug filters:
```

```
Conditional debug features:
```

```
firepower# PKI[13]: crypto_parsepkcs12, pki_oss1_pkcs12.c:1484
```

```
PKI[13]: pki_unpack_p12, pki_oss1_pkcs12.c:1414
```

```
PKI[4]: Error unpacking pkcs7 encrypted data
```

```
PKI[1]: error:060A60A3:digital envelope routines:FIPS_CIPHERINIT:disabled for fips in fips_enc.c line 1
```

```
PKI[1]: error:06074078:digital envelope routines:EVP_PBE_CipherInit:keygen failure in evp_pbe.c line 20
```

```
PKI[1]: error:23077073:PKCS12 routines:PKCS12_pbe_crypt:pkcs12 algor cipherinit error in p12_decr.c lin
```

```
PKI[1]: error:2306A075:PKCS12 routines:PKCS12_item_decrypt_d2i:
```

pkcs12 pbe crypt error

in p12_decr.c line 145.
PKI[4]:

pkcs7 encryption algorithm may not be fips compliant

PKI[4]: Error unpacking pkcs12 struct to extract keys and certs
PKI[13]: label: FTDv_C_cert
PKI[13]: TP list is NULL
PKI[13]: label: FTDv_C_cert
PKI[13]: TP list label: FTDv_C_cert
PKI[14]: pki_ossl_set_cert_store_dirty, pki_ossl_certstore.c:38
PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:41
PKI[13]: label: FTDv_C_cert
PKI[13]: TP list label: FTDv_C_cert

Sie können mit OpenSSL auch bestätigen, dass das vorliegende PKCS#12 nicht konforme FIPS PBE-Algorithmen enthält.

<#root>

OpenSSL>

pkcs12 -info -in ftdv_C_.p12 -noout

Enter Import Password:
MAC Iteration 2048
MAC verified OK
PKCS7 Encrypted data:

pbeWithSHA1And40BitRC2-CBC

, Iteration 2048
Certificate bag
Certificate bag
PKCS7 Data
Shrouded Keybag:

pbeWithSHA1And3-KeyTripleDES-CBC

, Iteration 2048

In der vorherigen Ausgabe gibt es zwei PBE-Algorithmen, pbeWithSHA1And40BitRC2-CBC und pbeWithSHA1And3-KeyTripleDES-CBC, die die Zertifikate bzw. den privaten Schlüssel schützen. Die erste Version ist nicht FIPS-kompatibel.

Lösung

Die Lösung besteht darin, den PBE-SHA1-3DES-Algorithmus für den Schutz von Zertifikaten und privaten Schlüsseln zu konfigurieren. Im obigen Beispiel muss nur der Zertifikatalgorithmus geändert werden. Zuerst müssen Sie die Privacy-Enhanced Mail (PEM)-Version der

ursprünglichen PKCS#12-Datei mit OpenSSL erhalten.

```
<#root>
```

```
OpenSSL>
```

```
pkcs12 -in ftdv_C_.p12 -out ftdv_C_.pem
```

```
Enter Import Password:
```

```
MAC verified OK
```

```
Enter PEM pass phrase:
```

```
Verifying - Enter PEM pass phrase:
```

Zuletzt müssen Sie den folgenden Befehl mit dem FIPS-kompatiblen PBE-Algorithmus verwenden, der die im vorherigen Schritt erhaltene PEM-Datei verwendet, um eine brandneue PKCS#12-Datei zu generieren:

```
<#root>
```

```
OpenSSL>
```

```
pkcs12 -certpbe PBE-SHA1-3DES -export -in ftdv_C_.pem -out ftdv_C_FIPS_compliant.p12
```

```
Enter pass phrase for ftdv_C_.pem:
```

```
Enter Export Password:
```

```
Verifying - Enter Export Password:
```

```
unable to write 'random state'
```

 Anmerkung: Wenn auch der Algorithmus zum Schutz des privaten Schlüssels geändert werden muss, können Sie das -keypbe-Schlüsselwort gefolgt von PBE-SHA1-3DES an den gleichen Befehl anhängen: `pkcs12 -certpbe PBE-SHA1-3DES -keypbe PBE-SHA1-3DES -export -in -out -out <PKCS12-Zertifikatsdatei>`.

Verifizierung

Verwenden Sie denselben OpenSSL-Befehl, um Informationen über die PKCS#12-Dateistruktur abzurufen, um zu bestätigen, dass FIPS-Algorithmen verwendet werden:

```
<#root>
```

```
OpenSSL>
```

```
pkcs12 -info -in ftdv_C_FIPS_compliant.p12 -noout
```

```
Enter Import Password:
```

```
MAC Iteration 2048
```

MAC verified OK
PKCS7 Encrypted data:

pbewithSHA1And3-KeyTripleDES-CBC

, Iteration 2048
Certificate bag
Certificate bag
PKCS7 Data
Shrouded Keybag:

pbewithSHA1And3-KeyTripleDES-CBC

, Iteration 2048

PKI-Debugging zeigt die Ausgabe unten an, wenn die Zertifikatinstallation erfolgreich war.

```
PKI[13]: crypto_parsepkcs12, pki_oss1_pkcs12.c:1484
PKI[13]: pki_unpack_p12, pki_oss1_pkcs12.c:1414
PKI[13]: pki_unpack_bags, pki_oss1_pkcs12.c:1383
PKI[13]: pki_unpack_bag, pki_oss1_pkcs12.c:1313
PKI[13]: add_cert, pki_oss1_pkcs12.c:1284
PKI[13]: add_cert_node, pki_oss1_pkcs12.c:1187
PKI[13]: pki_unpack_bag, pki_oss1_pkcs12.c:1313
PKI[13]: add_cert, pki_oss1_pkcs12.c:1284
PKI[13]: add_cert_node, pki_oss1_pkcs12.c:1187
PKI[13]: pki_unpack_bags, pki_oss1_pkcs12.c:1383
PKI[13]: pki_unpack_bag, pki_oss1_pkcs12.c:1313
PKI[13]: add_key, pki_oss1_pkcs12.c:1252
PKI[13]: add_cert_node, pki_oss1_pkcs12.c:1187
PKI[14]: compare_key_ids, pki_oss1_pkcs12.c:1150
PKI[12]: transfer_p12_contents_to_asa, pki_oss1_pkcs12.c:375
PKI[13]: label: FTDv_C_FIPS_Compliant
PKI[13]: TP list is NULL
```

```
CRYPTO_PKI: examining router cert:
CRYPTO_PKI: issuerName=/O=Cisco/OU=TAC/CN=RootCA_C1117
CRYPTO_PKI: subjectname=/CN=ftdv/unstructuredName=C1117_DRIVERAP.driverap.com
CRYPTO_PKI: key type is RSAPKI[13]: GetKeyUsage, pki_oss1_pkcs12.c:278
```

```
CRYPTO_PKI: bitValue of ET_KEY_USAGE = a0
CRYPTO_PKI: Certificate Key Usage = GENERAL_PURPOSE
CRYPTO_PKI: adding RSA Keypair
CRYPTO_PKI: adding as a router certificate.
CRYPTO_PKI: InsertCertData: subject name =
```

```
30 3b 31 0d 30 0b 06 03 55 04 03 13 04 66 74 64 76 31 2a 30
28 06 09 2a 86 48 86 f7 0d 01 09 02 16 1b 43 31 31 31 37 5f
44 52 49 56 45 52 41 50 2e 64 72 69 76 65 72 61 70 2e 63 6f
6d
```

```
CRYPTO_PKI: InsertCertData: issuer name =
```

```
30 35 31 0e 30 0c 06 03 55 04 0a 13 05 43 69 73 63 6f 31 0c
30 0a 06 03 55 04 0b 13 03 54 41 43 31 15 30 13 06 03 55 04
03 0c 0c 52 6f 6f 74 43 41 5f 43 31 31 31 37
```

```
CRYPTO_PKI: InsertCertData: serial number = 16 | .
```

```
CRYPTO_PKI: looking for cert in handle=0x00002abdc8cac50, digest=
```

aa 49 1e c2 c1 d5 30 60 4a 88 57 c8 3d 4e 3c 1c | .I....0`J.W.=N<.

CRYPTO_PKI: Cert record not found, returning E_NOT_FOUND
CRYPTO_PKI: Inserted cert into list.PKI[14]: pki_ossl_set_cert_store_dirty, pki_ossl_certstore.c:38
PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:41
PKI[9]: Cleaned PKI cache successfully
PKI[9]: Starting to build the PKI cache
PKI[4]: No identity cert found for TP: FTDv_C_FIPS_Compliant
PKI[4]: Failed to cache certificate chain for the trustpoint FTDv_C_FIPS_Compliant or none available
PKI[13]: CERT_GetTrustedIssuerNames, vpn3k_cert_api.c:1760
PKI[14]: map_status, vpn3k_cert_api.c:2229
PKI[4]: Failed to retrieve trusted issuers list or no trustpoint configured
PKI[13]: CERT_FreeTrustedIssuerNames, vpn3k_cert_api.c:1782
PKI[13]: crypto_pkcs12_add_sync_record, pki_ossl_pkcs12.c:144
PKI[13]: label: FTDv_C_FIPS_Compliant
PKI[13]: TP list label: FTDv_C_FIPS_Compliant

CRYPTO_PKI(Cert Lookup) issuer="cn=RootCA_C1117,ou=TAC,o=Cisco" serial number=16 | .

CRYPTO_PKI: looking for cert in handle=0x00002abdc8cac50, digest=
aa 49 1e c2 c1 d5 30 60 4a 88 57 c8 3d 4e 3c 1c | .I....0`J.W.=N<.

CRYPTO_PKI: ID cert in trustpoint FTDv_C_FIPS_Compliant successfully validated with CA cert.

CRYPTO_PKI: crypto_pki_authenticate_tp_cert()

CRYPTO_PKI: trustpoint FTDv_C_FIPS_Compliant authentication status = 0

CRYPTO_PKI: InsertCertData: subject name =

30 35 31 0e 30 0c 06 03 55 04 0a 13 05 43 69 73 63 6f 31 0c
30 0a 06 03 55 04 0b 13 03 54 41 43 31 15 30 13 06 03 55 04
03 0c 0c 52 6f 6f 74 43 41 5f 43 31 31 31 37

CRYPTO_PKI: InsertCertData: issuer name =

30 35 31 0e 30 0c 06 03 55 04 0a 13 05 43 69 73 63 6f 31 0c
30 0a 06 03 55 04 0b 13 03 54 41 43 31 15 30 13 06 03 55 04
03 0c 0c 52 6f 6f 74 43 41 5f 43 31 31 31 37

CRYPTO_PKI: InsertCertData: serial number = 01 | .

CRYPTO_PKI: looking for cert in handle=0x00002abdc8cac50, digest=
17 9d 0e b0 15 9d cd a2 5a 01 95 bf c6 8c 4f 2e | Z.....0.

CRYPTO_PKI: Cert record not found, returning E_NOT_FOUND
CRYPTO_PKI: Inserted cert into list.PKI[14]: pki_ossl_set_cert_store_dirty, pki_ossl_certstore.c:38
PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:41
PKI[9]: Cleaned PKI cache successfully
PKI[9]: Starting to build the PKI cache

CRYPTO_PKI(Cert Lookup) issuer="cn=RootCA_C1117,ou=TAC,o=Cisco" serial number=16 | .

CRYPTO_PKI: looking for cert in handle=0x00002abdc8cac50, digest=
aa 49 1e c2 c1 d5 30 60 4a 88 57 c8 3d 4e 3c 1c | .I....0`J.W.=N<.

PKI[7]: Get Certificate Chain: number of certs returned=2
PKI[13]: CERT_GetDNbyBuffer, vpn3k_cert_api.c:993
PKI[14]: map_status, vpn3k_cert_api.c:2229
PKI[7]: Built trustpoint cache for FTDv_C_FIPS_Compliant
PKI[13]: CERT_GetTrustedIssuerNames, vpn3k_cert_api.c:1760
PKI[14]: map_status, vpn3k_cert_api.c:2229
PKI[9]: Added 1 issuer hashes to cache.
PKI[13]: CERT_FreeTrustedIssuerNames, vpn3k_cert_api.c:1782
PKI[13]: crypto_pkcs12_free_sync_record, pki_ossl_pkcs12.c:113

```

PKI[13]: label: FTDv_C_FIPS_Compliant
PKI[13]: TP list label: FTDv_C_FIPS_Compliant
PKI[13]: label: FTDv_C_FIPS_Compliant
PKI[13]: TP list label: FTDv_C_FIPS_Compliant
PKI[14]: pki_ossl_set_cert_store_dirty, pki_ossl_certstore.c:38
PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:41
PKI[13]: label: FTDv_C_FIPS_Compliant
PKI[13]: TP list label: FTDv_C_FIPS_Compliant

```

CRYPTO_PKI: certificate data

<omitted output>

CRYPTO_PKI: status = 0: failed to get extension from cert

CRYPTO_PKI: certificate data

<omitted output>

PKI[13]: label: FTDv_C_FIPS_Compliant

PKI[13]: TP list label: FTDv_C_FIPS_Compliant

Schließlich zeigt das FMC sowohl CA- als auch Identitätszertifikate an, sofern verfügbar:

The screenshot shows the Cisco Firepower Management Center (FMC) interface. The 'Certificates' tab is selected under the 'Devices' section. A table lists certificates for two devices: FTDv_B and FTDv_C. For FTDv_C, the certificate 'FTDv_C_FIPS_Compliant' is highlighted. A modal window titled 'CA Certificate' is open, showing the following details:

- Status: Available
- Serial Number: 01
- Issued By:
 - Common Name: RootCA_C1117
 - Organization Unit: TAC
 - Organization: Cisco
- Issued To:
 - Common Name: RootCA_C1117
 - Organization Unit: TAC
 - Organization: Cisco
- Public Key Type: RSA (2048 bits)
- Signature Algorithm: SHA256 with RSA Encryption
- Associated Trustpoints: FTDv_C_FIPS_Compliant

The bottom of the interface shows the last login time: 'Last login on Friday, 2020-10-23 at 00:15:37 AM from 10.31.124.34' and a 'How To' button.

Cisco Firepower Management

https://10.31.124.31:6005/ddd/#PKICertificate

OverviewAnalysisPolicies**Devices**ObjectsAMPIntelligence

Device ManagementNATVPNQoSPlatform SettingsFlexConfig**Certificates**

Add

Name	Domain	Enrollment Type	Status
FTDv_B			
selfsigned_cert	Global	Self-Signed	CA ID
FTD.driverap.com	Global	Manual	CA ID
FTDv_C			
FTDv_C_FIPS_Compliant	Global	PKCS12 file	CA ID

Identity Certificate

- Status : Available
- Serial Number : 16
- Issued By :
 - Common Name : RootCA_C1117
 - Organization Unit : TAC
 - Organization : Cisco
- Issued To :
 - Host Name : C1117_DRIVERAP.driverap.com
 - Common Name : ftdv
- Public Key Type : RSA (4096 bits)
- Signature Algorithm : SHA256 with RSA Encryption
- Associated Trustpoints : FTDv_C_FIPS_Compliant

Close

Last login on Friday, 2020-10-23 at 00:15:37 AM from 10.31.124.34

How To

Activate Windows
Go to Settings to activate Windows

Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.