

IOS XRガイドンス – Mudhraルートおよび中間認証局に対する緊急不信

内容

概要

証明書のチェックや修復手順など、Cisco IOS XRルータでのeMudhra証明書の漏洩を特定して軽減する方法を説明します。

背景説明

このドキュメントでは、Cisco IOS XRを実行しているCiscoサービスプロバイダーのルーティングプラットフォームに関する、次の運用ガイドンスと暫定的な緩和手順について説明します。

- Cisco ASR 9000シリーズ
- Cisco 8000 シリーズ
- Cisco NCS 1000 シリーズ
- Cisco NCS 4000 シリーズ
- Cisco NCS 5500 シリーズ
- Cisco NCS 6000 シリーズ
- Cisco NCS 540/560シリーズ
- Cisco XRV 9000

これらの手順は、[Cisco Security Advisory cisco-sa-emudhra-info-ScS22A1r](#)に記載されているように、侵害されたeMudhra認証局に関連する潜在的な侵害に対処するものです。

この記事では、IOS XR Linux証明書ストアで関連する証明書を識別し、潜在的な問題を評価し、必要に応じて暫定的な緩和手順を適用する方法について説明します。

脆弱性と脅威のコンテキスト

2026年10月17日から10月20日の間に、Mudhraにおいて2025年4月のKey Generation Ceremony(KGC)において、前例のない暗号不具合が公開されました。キー生成中のランダム性の破綻により、8つのMudhra中間認証局（6つのTLS発行CAと2つのコード署名CA）の秘密キーが、数秒以内に不正な攻撃者によって因数分解され、導出される可能性があります。

重要な複合要素（Sectigoクロスシグニチャ）:2025年5月、侵害された8つの中間CAすべてが、Sectigoのレガシールート（AAA証明書サービス）によってクロスサインされました。Sectigoのルートはパブリックおよびエンタープライズの信頼ストアにユビキタスに組み込まれているため、侵害された中間CAによって発行された証明書は、ネイティブのeMudhraルートがなくても、デフォルトでオペレーティングシステムとTLSスタック全体でグローバルに信頼されます。

Cisco IOS XR証明書アーキテクチャおよび公開分析

IOS XRアプリケーションは、デフォルトでXR証明書ストアを使用します。IOS XR Linux CAバンドルには2つのeMudhra証明書が含まれています。これらは、次の3つの特定のシナリオでのみ使用されます。

- Linuxのコマンドラインを使用して、HTTPSサーバに対してcurlまたはwgetを実行します
- LDAPはTLS経由でアクセスされる
- Opflexを実装 (ASR 9000シリーズのみ)

設定されたトラストポイントと証明書の監査および特定

26.4.1より前のすべてのCisco IOS XRバージョン (2026年11月30日リリース予定) には、これらのCA証明書が含まれています。これらの証明書がXRデバイスに存在することを確認するには、XR Linux CLIにアクセスし、certificates.confファイルの内容を確認します。

```
<#root>
```

```
RP/0/RP0/CPU0:Router#
```

```
run
```

```
[xr-vm_node0_RP0_CPU0:~]$
```

```
grep "Comodo_AAA_Services_root.crt\|emSign_ECC_Root_CA_-_G3.crt" /etc/ca-certificates.conf
```

```
mozilla/Comodo_AAA_Services_root.crt
```

```
mozilla/emSign_ECC_Root_CA_-_G3.crt
```

証明書に1つまたは両方の証明書が記載されている場合は、両方のファイルのパスを探します。

```
<#root>
```

```
[xr-vm_node0_RP0_CPU0:~]$
```

```
find / -type f \( -name "Comodo_AAA_Services_root.crt" -o -name "emSign_ECC_Root_CA_-_G3.crt" \) 2>/dev/null
```

```
/usr/share/ca-certificates/mozilla/Comodo_AAA_Services_root.crt
```

```
/usr/share/ca-certificates/mozilla/emSign_ECC_Root_CA_-_G3.crt
```

これらのファイルが存在し、certificates.confで参照されている場合、デバイスが悪用される可能性があります。

修復手順

緩和手順は次の要素で構成されます。

- すべてのcertificate.confファイルの先頭に！を追加します
- 見つかった証明書の削除
- certificate.confファイルの更新

eXRリリース：

すべてのcertificate.confファイルの先頭に！を追加します

<#root>

```
[xr-vm_node0_RP0_CPU0:~]$
```

```
cat /etc/ca-certificates.conf | grep "Comodo_AAA_Services_root.crt\|emSign_ECC_Root_CA_-_G3.crt
```

```
!mozilla/Comodo_AAA_Services_root.crt
```

```
!mozilla/emSign_ECC_Root_CA_-_G3.crt
```

見つかった証明書の削除

<#root>

```
[xr-vm_node0_RP0_CPU0:~]$
```

```
rm /usr/share/ca-certificates/mozilla/Comodo_AAA_Services_root.crt
```

```
[xr-vm_node0_RP0_CPU0:~]$
```

```
rm /usr/share/ca-certificates/mozilla/emSign_ECC_Root_CA_-_G3.crt
```

certificate.confファイルの更新

<#root>

```
[xr-vm_node0_RP0_CPU0:~]$update-ca-certificates
```

```
Updating certificates in /etc/ssl/certs...
```

```
rehash: warning: skipping ca-certificates.crt,it does not contain exactly one certificate or CRL  
0 added,
```

```
2 removed;
```

```
done.
```

この手順は簡単ですが、すべてのVM（各ノードのdefault-sdrおよびsysadmin）とルータのホストOSで繰り返す必要があります。

この手順は、シェルスクリプトを実行することで自動化できます。

- アクティブRPの管理VMにスクリプトをアップロードしてコピーします。

<#root>

sysadmin-vm:0_RP0#

copy harddisk:exr_remove_eMudhra_cert.sh harddisk: location 0/RP0/CPU0/VM1

Tue Oct 27 01:59:29.149 UTC+00:00

Copying harddisk:exr_remove_eMudhra_cert.sh to harddisk:

exr_remove_eMudhra_cert.sh 100% 1604 4.3MB/s 00:00

File copied successfully

- アクティブRPの管理VMに移動します。

<#root>

RP/0/RP0/CPU0:Router#

admin

Last login: Mon Oct 26 22:46:01 2026 from 192.0.2.4

user connected from 192.0.2.4 using ssh on sysadmin-vm:0_RP0

sysadmin-vm:0_RP0#

run

[sysadmin-vm:0_RP0:~]\$

- スクリプトの実行

<#root>

[sysadmin-vm:0_RP0:~]\$.

/exr_remove_eMudhra_cert.sh

== Local sysadmin VM (sysadmin-vm:0_RP0) ==

-- /etc/ca-certificates.conf entries:

!mozilla/Comodo_AAA_Services_root.crt

!mozilla/emSign_ECC_Root_CA_-_G3.crt

found: /usr/share/ca-certificates/mozilla/Comodo_AAA_Services_root.crt

deleted: /usr/share/ca-certificates/mozilla/Comodo_AAA_Services_root.crt

found: /usr/share/ca-certificates/mozilla/emSign_ECC_Root_CA_-_G3.crt

deleted: /usr/share/ca-certificates/mozilla/emSign_ECC_Root_CA_-_G3.crt

--

Validation (expect: ls: cannot access '/etc/ssl/certs/...pem': No such file or directory):

ls: cannot access '/etc/ssl/certs/Comodo_AAA_Services_root.pem': No such file or directory

ls: cannot access '/etc/ssl/certs/emSign_ECC_Root_CA_-_G3.pem': No such file or directory

== Local host (my_host) ==

-- /etc/ca-certificates.conf entries:

!mozilla/Comodo_AAA_Services_root.crt

!mozilla/emSign_ECC_Root_CA_-_G3.crt

found: /usr/share/ca-certificates/mozilla/Comodo_AAA_Services_root.crt

deleted: /usr/share/ca-certificates/mozilla/Comodo_AAA_Services_root.crt

found: /usr/share/ca-certificates/mozilla/emSign_ECC_Root_CA_-_G3.crt

deleted: /usr/share/ca-certificates/mozilla/emSign_ECC_Root_CA_-_G3.crt

-- Validation (expect: ls: cannot access '/etc/ssl/certs/...pem': No such file or directory):

ls: cannot access '/etc/ssl/certs/Comodo_AAA_Services_root.pem': No such file or directory

ls: cannot access '/etc/ssl/certs/emSign_ECC_Root_CA_-_G3.pem': No such file or directory

== lc0_xr ==

-- /etc/ca-certificates.conf entries:

!mozilla/Comodo_AAA_Services_root.crt

!mozilla/emSign_ECC_Root_CA_-_G3.crt

found: /usr/share/ca-certificates/mozilla/emSign_ECC_Root_CA_-_G3.crt

deleted: /usr/share/ca-certificates/mozilla/emSign_ECC_Root_CA_-_G3.crt

found: /usr/share/ca-certificates/mozilla/Comodo_AAA_Services_root.crt

deleted: /usr/share/ca-certificates/mozilla/Comodo_AAA_Services_root.crt

-- Validation (expect: ls: cannot access '/etc/ssl/certs/...pem': No such file or directory):

ls: cannot access '/etc/ssl/certs/Comodo_AAA_Services_root.pem': No such file or directory

ls: cannot access '/etc/ssl/certs/emSign_ECC_Root_CA_-_G3.pem': No such file or directory

== rp0_xr ==

-- /etc/ca-certificates.conf entries:

!mozilla/Comodo_AAA_Services_root.crt

!mozilla/emSign_ECC_Root_CA_-_G3.crt

found: /usr/share/ca-certificates/mozilla/Comodo_AAA_Services_root.crt

deleted: /usr/share/ca-certificates/mozilla/Comodo_AAA_Services_root.crt

found: /usr/share/ca-certificates/mozilla/emSign_ECC_Root_CA_-_G3.crt

deleted: /usr/share/ca-certificates/mozilla/emSign_ECC_Root_CA_-_G3.crt

-- Validation (expect: ls: cannot access '/etc/ssl/certs/...pem': No such file or directory):

ls: cannot access '/etc/ssl/certs/Comodo_AAA_Services_root.pem': No such file or directory

```
ls: cannot access '/etc/ssl/certs/emSign_ECC_Root_CA_-_G3.pem': No such file or directory
Done.
```

すべてのVMとホストOSで、証明書名がcertificates.confにコメント化され、証明書が削除および更新されます。

スクリプトリンク : <https://cisco.box.com/s/mevtcydjarl2tz0rc39862x100b8x3mu>

XR7リリース :

XR7リリースの手順については、現在検討中です。

参考資料

1. [Ciscoセキュリティアドバイザリ : cisco-sa-emudhra-info-ScS22A1r](#)
2. [Cisco Talosブログ : 侵害されたeMudhra中間証明書](#)

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。