Cisco ASA ソフトウェアの多重 脆弱点

Critical

アドバイザリーID : cisco-sa-20141008-asa

初公開日 : 2014-10-08 16:00

最終更新日 : 2015-07-09 15:14

バージョン 3.0 : Interim

CVSSスコア : 9.0

回避策 : No Workarounds available

Cisco バグ ID : CSCul36176 CSCum00556 CSCum96401 CSCuq29136 CSCtq52661 CSCuo68327 CSCuq28582 CSCum46027 CSCun11074 CSCum56399 CSCup36829 CSCuq47574 CSCun10916 CSCuq41510

CVE-2014-3389
CVE-2014-3387
CVE-2014-3388
CVE-2014-3392
CVE-2014-3382
CVE-2014-3393
CVE-2014-3390
CVE-2014-3391
CVE-2014-3385
CVE-2014-3386
CVE-2014-3383
CVE-2014-3394
CVE-2014-3384

概要

2015-July-08 アップデート: Cisco PSIRT は CVE-2014-3383 から影響を受ける Cisco ASA デバイスを持つ何人かの Cisco カスタマに中断にこの Security Advisory で表われた Cisco ASA VPN サービス拒否の脆弱性気づいています。 中断を引き起こすトラフィックにより特定のソース IPv4 アドレスに分離されました。 Cisco はトラフィックが悪意のある意図無しで送信 されたことをプロバイダおよびオーナーをそのデバイスのおよび判別される実行しました。 Cisco は remediate に Cisco 固定 ASA ソフトウェア リリースにことを顧客アップグレードこの問題強く推奨します。

Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェアは次の脆弱性から影響を受けます:

- SQL*NET（Oracle） Cisco ASA インスペクション エンジン サービス拒否の脆弱性
- Cisco ASA VPN サービス拒否の脆弱性
- Cisco ASA IKEv2 サービス拒否の脆弱性
- Cisco ASA 健全性およびパフォーマンスモニタ サービス拒否の脆弱性
- Cisco ASA GPRS Tunneling Protocol（GTP） インスペクション エンジン サービス拒否の脆弱性
- Cisco ASA SunRPC インスペクション エンジン サービス拒否の脆弱性
- Cisco ASA DNS インスペクション エンジン サービス拒否の脆弱性
- Cisco ASA VPN Failover コマンド インジェクト脆弱性
- Cisco ASA VNMC コマンド 入力 検証脆弱性
- Cisco ASA ローカル パス包含脆弱性
- Cisco ASA Clientless SSL VPN 情報の漏えいおよびサービス拒否の脆弱性
- Cisco ASA Clientless SSL VPN 門脈カスタマイゼーション 統合脆弱性
- Cisco ASA Smart Call Home デジタル認証 検証脆弱性

これらの脆弱性は互いの依存しないです; いずれかの脆弱性の影響を受けるリリースであっても、他の脆弱性の影響は受けない場合があります。

GPRS Tunneling Protocol（GTP） SQL*NET（Oracle） Cisco ASA インスペクション エンジン サービス拒否の脆弱性、Cisco ASA VPN サービス拒否の脆弱性、Cisco ASA IKEv2 サービス拒否の脆弱性、Cisco ASA 健全性およびパフォーマンスモニタ サービス拒否の脆弱性、Cisco ASA インスペクション エンジン サービス拒否の脆弱性、Cisco ASA SunRPC インスペクション エンジン サービス拒否の脆弱性および Cisco ASA DNS インスペクション エンジン サービス拒否の脆弱性の不正利用の成功はサービス拒否 （DoS）に状態を導く影響を受けたデバイスのリロードという結果に終るかもしれません。

Cisco ASA VPN Failover コマンド インジェクト脆弱性、Cisco ASA VNMC コマンド 入力 検証脆弱性および Cisco ASA ローカル パス包含脆弱性の不正利用の成功は影響を受けたシステムの完全な妥協という結果に終るかもしれません。

Cisco ASA Clientless SSL VPN 情報の漏えいおよびサービス拒否の脆弱性の不正利用の成功は内部情報の公開か、場合によっては、影響を受けたシステムのリロードという結果に終るかもしれません。

Cisco ASA Clientless SSL VPN 門脈カスタマイゼーション 統合脆弱性の不正利用の成功は原因となるかもしれない Clientless SSL VPN ポータルの妥協という結果に、信任状の窃盗、または悪意のある Webページにユーザのリダイレクトはクロスサイト スクリプティング（XSS）に制限されない不正侵入の複数の型の終るかもしれません。

Cisco ASA Smart Call Home デジタル認証 検証脆弱性の不正利用の成功は攻撃者がデジタル認証認証をバイパスし、リモートアクセス VPN によってネットワークか影響を受けたシステムへの Cisco 適応性がある安全 装置管理（ASDM）によって管理アクセスの中でアクセス権を得ることを可能にする可能性があるデジタル認証 検証バイパスという結果に終るかもしれません。

シスコはこれらの脆弱性に対処するソフトウェア アップデートを提供しています。 この中のいくつかの脆弱性には影響を軽減する回避策が存在します。

このアドバイザリは、次のリンクより確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20141008-asa

該当製品

以下の製品で動作する Cisco ASA ソフトウェアは多重 脆弱点から影響を受けます:

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Cisco ASA 5500-X シリーズ次世代ファイアウォール
- Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータのための Cisco ASA サービス モジュール
- Cisco ASA 1000V クラウド ファイアウォール
- Cisco 適応型セキュリティ仮想アプライアンス（ASAv）（ASAv）

Cisco ASA ソフトウェアの該当するリリースは特定の脆弱性によって変わります。 該当するリリースに関する詳細についてはこの Security Advisory の「ソフトウェア バージョン および 修正」セクションを参照して下さい。

脆弱性のある製品

SQL*NET（Oracle）Cisco ASA インスペクション エンジン サービス拒否の脆弱性

Cisco ASA ソフトウェアはこの脆弱性から SQL*Net インスペクションがイネーブルになっている場合影響を受けます。

SQL*Net インスペクションがイネーブルになっているかどうか判別するために、 **show service ポリシーを**使用して下さい **| sqlnet** コマンドを **含み、**出力が戻ることを確認して下さい。 次の例は SQL*Net インスペクションがイネーブルの状態で Cisco ASA ソフトウェアを示したものです:

```
ciscoasa# show service-policy | include sqlnet
Inspect: sqlnet, packet 0, drop 0, reset-drop 0
```

注: SQL*Net インスペクションはデフォルトでイネーブルになっています。

Cisco ASA VPN サービス拒否の脆弱性

Cisco ASA ソフトウェアはこの脆弱性から IKEv1 および IKEv2 VPN 接続を終えるためにシステムが設定される場合影響を受けます。 これには IPSec VPN クライアントおよび IKEv2 AnyConnect VPN、および L2TP Over IPSec VPN 接続によって両方 LAN-to-LAN、リモートアクセス VPN が含まれています。 Clientless または AnyConnect SSL VPN はこの脆弱性から影響を受けません。

Cisco ASA が IKEv1 または IKEv2 VPN 接続を終えるために設定されたかどうか確認するためにクリプト マップは少なくとも 1 つのインターフェイスのために設定する必要があります。 管理者は **show running-config クリプト マップを**使用する必要があります **| interface コマンドを含み、**出力を戻すことを確認して下さい。 次の例は *outside インターフェイス*で設定される *cmap* と呼ばれるクリプト マップを示したものです:

```
ciscoasa# show running-config crypto map | include interface
crypto map outside_map interface outside
```

注: IKEv1 か IKEv2 VPN はデフォルトで設定されません。

Cisco ASA IKEv2 サービス拒否の脆弱性

Cisco ASA ソフトウェアはこの脆弱性から IKEv2 VPN 接続を終えるためにシステムが設定される場合影響を受けます。 これには LAN-to-LAN IKEv2 および AnyConnect IKEv2 VPN 接続が含まれています。 IKEv2 VPN がイネーブルになった使用 **show running-config 暗号 ikev2** であるかどうか判別するため **| enable コマンドを含み、**コマンドが出力を戻すことを確認して下さい。 次の例はインターフェイス *外部*でイネーブルになっている IKEv2 VPN の Cisco ASA を示したものです:

```
ciscoasa# show running-config crypto ikev2 | include enable
crypto ikev2 enable outside
```

IKEv2 をイネーブルになっていてもらうことに加えて Cisco ASA は IKEv2 がイネーブルになっているインターフェイスで設定されるクリプト マップがある必要があります。 これは **show running-config クリプト マップの**使用によって判別することができます **| interface コマンド**および出力を戻すことを確認することを **含んで下さい。** 次の例は *outside インターフェイス*で設定される *cmap* と呼ばれるクリプト マップを示したものです:

```
ciscoasa# show running-config crypto map | include interface
crypto map outside_map interface outside
```

注: IKEv2 VPN はデフォルトでイネーブルになっていません。

Cisco ASA 健全性およびパフォーマンスモニタ サービス拒否の脆弱性

Cisco ASA ソフトウェアはこの脆弱性から ASDM のための健全性およびパフォーマンスの監視 (HPM) がイネーブルになっている場合影響を受けます。

HPM がイネーブルになっているかどうか判別するために、 **show running-config を**使用して下さい **| hpm** コマンドを **含み、**出力が戻ることを確認して下さい。 次の例は HPM 機能がイネ

ーブルの状態で Cisco ASA ソフトウェアを示したものです:

```
ciscoasa# show running-config | include hpm
ciscoasa# hpm topn enable
```

注: HPM はデフォルトでイネーブルになっていません。

Cisco ASA GPRS Tunneling Protocol（GTP）インスペクション エンジン サービス拒否の脆弱性

Cisco ASA ソフトウェアはこの脆弱性から GPRS Tunneling Protocol（GTP）（GTP）インスペクションがイネーブルになっている場合影響を受けます。

GTP インスペクションがイネーブルになっているかどうか判別するために、 **show service ポリシーを**使用して下さい **| gtp** コマンドを **含み、**出力が戻ることを確認して下さい。 次の例は GTP インスペクションがイネーブルの状態で Cisco ASA ソフトウェアを示したものです:

```
ciscoasa# show service-policy | include gtp
Inspect: gtp, packet 0, drop 0, reset-drop 0
```

注: GTP インスペクションはデフォルトでイネーブルになっていません。

Cisco ASA SunRPC インスペクション エンジン サービス拒否の脆弱性

Cisco ASA ソフトウェアはこの脆弱性から SunRPC インスペクションがイネーブルになっている場合影響を受けます。

SunRPC インスペクションがイネーブルになっているかどうか判別するために、 **show service ポリシーを**使用して下さい **| sunrpc** コマンドを **含み、**出力が戻ることを確認して下さい。 次の例は SunRPC インスペクションがイネーブルの状態で Cisco ASA ソフトウェアを示したものです:

```
ciscoasa# show service-policy | include sunrpc
Inspect: sunrpc, packet 0, drop 0, reset-drop 0
```

注: SunRPC インスペクションはデフォルトでイネーブルになっています。

Cisco ASA DNS インスペクション エンジン サービス拒否の脆弱性

Cisco ASA ソフトウェアはこの脆弱性から DNS インスペクションがイネーブルになっている場合影響を受けます。

DNS インスペクションがイネーブルになっているかどうか判別するために、 **show service ポリシーを**使用して下さい **| dns** コマンドを **含み、**出力が戻ることを確認して下さい。 次の例は DNS インスペクションがイネーブルの状態で Cisco ASA ソフトウェアを示したものです:

```
ciscoasa# show service-policy | include dns
```

```
Inspect: dns preset_dns_map, packet 0, drop 0, reset-drop 0, v6-fail-close 0
```

注: DNS インスペクションはデフォルトでイネーブルになっています。

Cisco ASA VPN Failover コマンド インジェクト脆弱性

Cisco ASA ソフトウェアはこの脆弱性から VPN 接続の型を、Clientless SSL VPN を除く終えるためにシステムが設定され高可用性の（HA）モードで設定されれば場合影響を受けます（別名フェールオーバー モード）。

管理者は **show running-config クリプト マップを**使用できます **|** どのタイプの IKEv1 または IKEv2 IPSec VPN でもシステムおよび **show running-config webvpn** で設定されるかどうか確認する **interface コマンドを含んで下さい |** AnyConnect SSL VPN が設定されるかどうか確認する **anyconnect** コマンドを **含んで下さい。** 次の例は IPSec および AnyConnect 両方 SSL VPN が設定されている Cisco ASA を示したものです:

```
ciscoasa# show running-config webvpn | include anyconnect enable
 anyconnect enable
ciscoasa# show run crypto map | include interface
 crypto map outside_map interface outside
```

管理者は **show failover コマンドを**使用し、フェールオーバーが高可用性のモードが設定されたかどうか確認することついていることを確認できます。 次の例は高可用性のモードがイネーブルの状態で Cisco ASA を示したものです:

```
ciscoasa# show failover
Failover On
[...]
```

注: この脆弱性はフェールオーバー トラフィックを保護するのに Failover 鍵を使用しない HA 設定だけ影響を与えます。 HA および VPN はデフォルトでイネーブルになっていません。

Cisco ASA VNMC コマンド 入力 検証脆弱性

影響を受けたソフトウェアのバージョンを実行するすべての Cisco ASA はこの脆弱性から影響を受けます。

Cisco ASA ローカル パス包含脆弱性

影響を受けたソフトウェアのバージョンを実行するすべての Cisco ASA はこの脆弱性から影響を受けます。

Cisco ASA Clientless SSL VPN 情報の漏えいおよびサービス拒否の脆弱性

Cisco ASA ソフトウェアはこの脆弱性から Clientless SSL VPN ポータルがイネーブルになっている場合影響を受けます。 Clientless SSL VPN ポータルがイネーブルになった使用 **show running-config webvpn** コマンド判別しである、webvpn が少なくとも 1 つのインターフェイス

でイネーブルになっていることを確認するためかどうか。 次の例は *outside インターフェイス*の Clientless SSL VPN 門脈イネーブルになったのの Cisco ASA を示したものです:

```
ciscoasa# show running-config webvpn
webvpn
 enable outside
 [...]
```

注: Clientless SSL VPN ポータルはデフォルトでイネーブルになっていません。

Cisco ASA Clientless SSL VPN 門脈カスタマイゼーション 統合脆弱性

Cisco ASA ソフトウェアはこの脆弱性から次の条件が満たされる場合影響を受けます:

1. Clientless SSL VPN 門脈機能はイネーブルになっています
2. Clientless SSL VPN ポータルのためのデフォルト カスタマイゼーション オブジェクトか新しく作成されたカスタマイゼーション オブジェクトは ASDM で下検分されなければなりません

Clientless SSL VPN ポータルがイネーブルになった使用 **show running-config webvpn** コマンド判別しである、webvpn が 1 つのインターフェイスで少なくともイネーブルになっていることを確認するためかどうか。 次の例は *outside インターフェイス*の Clientless SSL VPN 門脈イネーブルになったのの Cisco ASA を示したものです:

```
ciscoasa# show running-config webvpn
webvpn
 enable outside
 [...]
```

カスタマイゼーション オブジェクトのプレビューが行われたかどうか確認する方式がありません。 次の方式がカスタマイゼーション オブジェクトを下検分するのに使用されています。 **CLIENTLESS SSL VPN アクセス**への ASDM ナビゲート **- > PORTAL - > カスタマイゼーション- > プレビュー**。

Cisco ASA Clientless SSL VPN 門脈カスタマイゼーション 統合脆弱性のための妥協の追加インジケータ

脆弱な設定を実行している顧客は門脈カスタマイゼーションが妥協されなかったことを確認する必要があります。 顧客はポータルがカスタマイゼーション オブジェクトを工クスポートし、手動でオブジェクトが悪意のあるコードが含まれていないことを確認することことをによって妥協されなかったことを確認できます。

新しいカスタム オブジェクトおよびデフォルト カスタマイゼーション オブジェクト（DfltCustomization）は分析する必要があります。 SSL VPN 門脈カスタマイゼーション オブジェクトをエクスポートするために、エクスポートされる *<object name>* が SSL VPN 門脈カスタマイゼーション オブジェクトの名前である *<dest fname>* がカスタマイゼーション オブジェクトのコピーを含むファイルの名前である **エクスポート webvpn カスタマイゼーション <object name> <dest fname>** コマンドを使用すれば。

次の例に *Customization_to_verify* と呼ばれるファイルにデフォルト カスタマイゼーション オブジェクト *DfltCustomization* をエクスポートする方法を示されています

```
ciscoasa# export webvpn customization DfltCustomization Customization_to_verify
```

Customization_to_verify ファイルはデバイス ディスクで保存され、更なる分析のために エクスポートすることができます。

顧客はシステムにあるカスタマイゼーション オブジェクトすべてのためのこのプロセスを繰り返す必要があります。

Cisco ASA Smart Call Home デジタル認証 検証脆弱性

Cisco ASA ソフトウェアはこの脆弱性から Smart Call Home （SCH）機能がシステムで設定されるか、または設定されたら影響を受けます。 機能が設定されるとき、*_SmartCallHome_ServerCA* と呼ばれるデジタル認証 トラストポイントはシステムで自動的にインストールされています。 このトラストポイントがインストールされているかどうか判別するために、 **show running-config crypto ca trustpoint _SmartCallHome_ServerCA** コマンドを使用し、出力を戻すことを確認して下さい。 次の例はインストールされるこのトラストポイントの Cisco ASA を示したものです:

```
ciscoasa# show running-config crypto ca trustpoint _SmartCallHome_ServerCA
crypto ca trustpoint _SmartCallHome_ServerCA
 crl configure
```

注: このトラストポイントの存在はシステムを脆弱にします; ただし、この脆弱性は設定されるデジタル証明書 検証サービスに頼るもう一つの機能がなければ不正利用することができません。 これらの機能の例は VPN のためのデジタル認証認証か ASDM 接続または TLS プロキシおよび電話プロキシです。 SCH はデフォルトでイネーブルになっていません。

脆弱性を含んでいないことが確認された製品

他のシスコ製品においてこのアドバイザリの影響を受けるものは、現在確認されていません。

詳細

Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェアは Cisco Catalyst 6500 シリーズ スイッチに Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス、Cisco ASA 5500-X 次世代ファイアウォール、Cisco ASA サービス モジュール（ASASM）および Cisco 7600 シリーズ ルータによって、Cisco ASA 1000V クラウド ファイアウォール、および Cisco 適応型セキュリティ仮想アプライアンス（ASAv）使用するオペレーティング システムです（ASAv）。 Cisco ASA ファミリーはファイアウォール、侵入防御システム（IPS）、反X のようなネットワークセキュリティサービスを、および VPN 提供します。

SQL*NET（Oracle） Cisco ASA インスペクション エンジン サービス拒否の脆弱性

SQL*Net インスペクション エンジン コードの脆弱性はリモート攻撃者非認証により影響を受けたシステムのリロードを引き起こすようにする可能性があります。

脆弱性は巧妙に細工された SQL リダイレクト パケットの不適当な処理が原因です。 攻撃者は影響を受けたシステムを通してリダイレクト パケットの巧妙に細工されたシーケンスの送信によってこの脆弱性を不正利用する可能性があります。

注: Cisco ASA SQL*Net インスペクション エンジンによって検査されるトランジットトラフィックだけこの脆弱性を不正利用するのに使用することができます。 この脆弱性は単一およびマルチ コンテキスト モードのルーティングされたおよび透過ファイアウォール モード影響を与えます。 この脆弱性は IPバージョン 4 （IPv4）および IP バージョン 6(IPv6) トラフィックによって引き起こすことができます。

この脆弱性 Cisco バグ ID CSCum46027 （ 登録ユーザのみ ）で文書化されています、よくある脆弱性および公開（CVE） ID CVE-2014-3382 は割り当てられました。

Cisco ASA VPN サービス拒否の脆弱性

Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェアの IKE コードの脆弱性はリモート攻撃者非認証により影響を受けたシステムのリロードを引き起こすようにする可能性があります。

脆弱性は UDP パケットの不十分な検証が原因です。 攻撃者は影響を受けたシステムへ巧妙に細工された UDP パケットを送信 することによってこの脆弱性を不正利用する可能性があります。 エクスプロイトは攻撃者により影響を受けたシステムのリロードを引き起こすことを可能にする可能性があります。

注: 本脆弱性を不正利用する目的で使用できるのは、該当システム宛てのトラフィックに限られます。 この脆弱性はルーティングされたファイアウォール モードだけと単一かマルチ コンテキスト モードで設定されるシステムに影響を及ぼします。 この脆弱性は IPバージョン 4 （IPv4）および IP バージョン 6(IPv6) トラフィックによって引き起こすことができます。

この脆弱性は Cisco バグ ID CSCul36176 （ 登録ユーザのみ ）で文書化されています、CVE ID CVE-2014-3383 を割り当てられました。

Cisco ASA IKEv2 サービス拒否の脆弱性

Cisco ASA ソフトウェアの IKEv2 コードの脆弱性はリモート攻撃者非認証により影響を受けたシステムのリロードを引き起こすようにする可能性があります。
脆弱性は巧妙に細工された IKEv2 パケットの不適当な処理が原因です。 攻撃者は IKEv2 トンネルの確立の間に巧妙に細工されたパケットの送信によってこの脆弱性を不正利用する可能性があります。 エクスプロイトは攻撃者により DoS 状態の原因となる影響を受けたシステムのリロードを引き起こすことを可能にする可能性があります

注: 本脆弱性を不正利用する目的で使用できるのは、該当システム宛てのトラフィックに限られま

す。 この脆弱性はルーティングされたファイアウォール モードだけと単一かマルチ コンテキスト モードで設定されるシステムに影響を及ぼします。 この脆弱性は IPv4 および IPv6 トラフィックによって引き起こすことができます。

この脆弱性は Cisco バグ ID CSCum96401 （ 登録ユーザのみ ）で文書化されています、CVE ID CVE-2014-3384 を割り当てられました。

Cisco ASA 健全性およびパフォーマンスモニタ サービス拒否の脆弱性

Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェアの ASDM 機能のための健全性およびパフォーマンスの監視（HPM）の脆弱性は非認証、リモート攻撃者により影響を受けたデバイスおよび終局サービス拒否 （DoS）状態のリロードを引き起こすことを可能にする可能性があります。

脆弱性は HPM 機能のオペレーションの競合状態が原因です。 攻撃者は影響を受けたデバイスを通って確立されるべき多数のハーフ・オープン同時接続の送信によってこの脆弱性を不正利用する可能性があります。 エクスプロイトは攻撃者により DoS 状態の原因となる可能性がある影響を受けたデバイスのリロードを引き起こすことを可能にする可能性があります。

注: 中継 TCPトラフィックだけこの脆弱性を不正利用するのに使用することができます。 この脆弱性は単一およびマルチ コンテキスト モードのルーティングされたおよび透過ファイアウォール モード影響を与えます。 この脆弱性は IPv4 および IPv6 トラフィックによって引き起こすことができます。

この脆弱性は Cisco バグ ID CSCum00556 （ 登録ユーザのみ ）で文書化されています、CVE ID CVE-2014-3385 を割り当てられました。

Cisco ASA GPRS Tunneling Protocol（GTP） インスペクション エンジン サービス拒否の脆弱性

Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェアのリモート攻撃者 GPRS Tunneling Protocol（GTP）（GTP）インスペクション エンジンの脆弱性は非認証により影響を受けたシステムのリロードを引き起こすようにする可能性があります。

脆弱性は特定のシーケンスで送信 されたとき GTP パケットの不適当な処理が原因です。 攻撃者は影響を受けたシステムを通して巧妙に細工された GTP パケットの送信によってこの脆弱性を不正利用する可能性があります。 エクスプロイトは攻撃者により影響を受けたシステムのリロードを引き起こすことを可能にする可能性があります

注: Cisco ASA GTP インスペクション エンジンによって検査されるトランジットトラフィックだけこの脆弱性を不正利用するのに使用することができます。 この脆弱性は単一およびマルチ コンテキスト モードのルーティングされたおよび透過ファイアウォール モード影響を与えます。 この脆弱性は IPv4 トラフィックによってしか引き起こすことができません。

この脆弱性は Cisco バグ ID CSCum56399 （ 登録ユーザのみ ）で文書化されています、CVE ID CVE-2014-3386 を割り当てられました。

Cisco ASA SunRPC インスペクション エンジン サービス拒否の脆弱性

Cisco 適応型セキュリティ アプライアンス (ASA) ソフトウェアの SunRPC インスペクション エンジンの脆弱性はリモート攻撃者非認証により影響を受けたシステムのリロードを引き起こすようにする可能性があります。

脆弱性は SunRPC 巧妙に細工されたパケットの不十分な検証が原因です。 攻撃者は影響を受けたシステムを通して SunRPC 巧妙に細工されたパケットの送信によってこの脆弱性を不正利用する可能性があります。 エクスプロイトは攻撃者により影響を受けたシステムのリロードを引き起こすことを可能にする可能性があります。

注: Cisco ASA SunRPC インスペクション エンジンによって検査されるトランジットトラフィックだけこの脆弱性を不正利用するのに使用することができます。 この脆弱性は単一およびマルチ コンテキスト モードのルーティングされたおよび透過ファイアウォール モード影響を与えます。 この脆弱性は IPv4 および IPv6 トラフィックによって引き起こすことができます。

この脆弱性は Cisco バグ ID CSCun11074 （ 登録ユーザのみ ）で文書化されています、CVE ID CVE-2014-3387 を割り当てられました。

Cisco ASA DNS インスペクション エンジン サービス拒否の脆弱性

Cisco 適応型セキュリティ アプライアンス (ASA) ソフトウェアの DNS インスペクション エンジンの脆弱性はリモート攻撃者非認証により影響を受けたシステムのリロードを引き起こすようにする可能性があります。
脆弱性は巧妙に細工された DNS パケットの不十分な検証が原因です。 攻撃者は影響を受けたシステムを通して巧妙に細工された DNS パケットの送信によってこの脆弱性を不正利用する可能性があります。 エクスプロイトは攻撃者により影響を受けたシステムのリロードを引き起こすことを可能にする可能性があります。

注: Cisco ASA DNS インスペクション エンジンによって検査されるトランジットトラフィックだけこの脆弱性を不正利用するのに使用することができます。 この脆弱性は単一およびマルチ コンテキスト モードのルーティングされたおよび透過ファイアウォール モード影響を与えます。 この脆弱性は IPv4 および IPv6 トラフィックによって引き起こすことができます。

この脆弱性は Cisco バグ ID CSCuo68327 （ 登録ユーザのみ ）で文書化されています、CVE ID CVE-2014-3388 を割り当てられました。

Cisco ASA VPN Failover コマンド インジェクト脆弱性

Cisco ASA ソフトウェアの VPN コードの脆弱性はフェールオーバー インターフェイスによってスタンバイユニットに設定コマンドを入れる認証される、リモート攻撃者可能にする可能性があります。 結果として、攻撃者はアクティブな、スタンバイ フェールオーバー ユニットの完全な制御を引き継げます可能性があります。

脆弱性は確立された VPN トンネルから来るパケットのための内部フィルタの不適当な実装が原因です。 攻撃者はフェールオーバー インターフェイス IP アドレスに送信された巧妙に細工されたパケットの送信によってこの脆弱性を不正利用する可能性があります。

注: 本脆弱性を不正利用する目的で使用できるのは、該当システム宛てのトラフィックに限られます。 この脆弱性はルーティングされたファイアウォール モードと単一かマルチ コンテキスト モードで設定されるシステムだけ影響を及ぼします。 この脆弱性は IPv4 および IPv6 トラフィックによって引き起こすことができます。

この脆弱性は Cisco バグ ID CSCuq28582 （ 登録ユーザのみ ）で文書化されています、CVE ID CVE-2014-3389 を割り当てられました。

Cisco ASA VNMC コマンド 入力 検証脆弱性

Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェアの Virtual Network Management Center （VNMC）ポリシー コードの脆弱性は *ルート ユーザ*の特権の根本的な Linux オペレーティング システムにアクセスする認証された、ローカル攻撃者を可能にする可能性があります。

脆弱性はユーザが指定する入力の不十分な sanitization が原因です。 攻撃者は管理者として影響を受けたシステムにログオンし、ディスクに悪意のあるスクリプトを不正利用するコピーしによってスクリプトを実行することこの脆弱性を、可能性があります。

注: 本脆弱性を不正利用する目的で使用できるのは、該当システム宛てのトラフィックに限られます。 この脆弱性は単一およびマルチ コンテキスト モードのルーティングされたおよび透過ファイアウォール モード影響を与えます。 デフォルト 設定では、管理はまたはこの脆弱性を不正利用するためアクセスが必要である 15 に特権を与えります。

この脆弱性は Cisco バグ ID CSCuq41510 （ 登録ユーザのみ ）および CSCuq47574 （ 登録ユーザのみ ）で文書化されています、CVE ID CVE-2014-3390 を割り当てられました。

Cisco ASA ローカル パス包含脆弱性

Cisco ASA ソフトウェアの環境変数を工クスポートする機能の脆弱性は悪意のあるライブラリをインジェクトし、システムの完全な制御を引き継ぐ認証された、ローカル攻撃者を可能にする可能性があります。

脆弱性は LD_LIBRARY_PATH 環境の不適当な設定が原因です。 攻撃者は影響を受けたシステム

の外部メモリに悪意のあるライブラリをコピーすることおよびシステムのリロードを引き起こすことによってこの脆弱性を不正利用する可能性があります。 エクスプロイトは攻撃者が悪意のあるライブラリをロードし、システムの完全な妥協の原因となる可能性がある根本的な Linux OS にアクセスするために影響を受けたシステムを強制することを可能にする可能性があります。

注: 本脆弱性を不正利用する目的で使用できるのは、該当システム宛てのトラフィックに限られます。 この脆弱性は単一およびマルチ コンテキスト モードのルーティングされたおよび透過ファイアウォール モード影響を与えます。 この脆弱性を不正利用するためにシステムのリロードは必要です。 デフォルト 設定では、管理はまたはこの脆弱性を不正利用するためアクセスが必要である 15 に特権を与えります。

この脆弱性は Cisco バグ ID CSCtq52661 （ 登録ユーザのみ ）で文書化されています、CVE ID CVE-2014-3391 を割り当てられました。

Cisco ASA Clientless SSL VPN 情報の漏えいおよびサービス拒否の脆弱性

Clientless SSL VPN 門脈機能の脆弱性はリモート攻撃者非認証がランダム記憶域にアクセスするようにする可能性があります。 この脆弱性が原因で、攻撃者はメモリの保存されている情報にアクセスでき、影響を受けたシステムのリロードに導く可能性があるメモリのこの部分を破損場合によってはできるかもしれません。

脆弱性はユーザが指定する入力の不十分な sanitization が原因です。 攻撃者は Clientless SSL VPN ポータルへのアクセスの間に渡されたパラメータの任意の値の設定によってこの脆弱性を不正利用する可能性があります。

注: 本脆弱性を不正利用する目的で使用できるのは、該当システム宛てのトラフィックに限られます。 この脆弱性はルーティングされたファイアウォール モードと単一コンテキスト モードでだけ設定されるシステムだけ影響を及ぼします。 この脆弱性は IPv4 および IPv6 トラフィックによって引き起こすことができます。 有効な TCP ハンドシェイクがこの脆弱性を不正利用するために必要となります。

この脆弱性は Cisco バグ ID CSCuq29136 （ 登録ユーザのみ ）で文書化されています、CVE ID CVE-2014-3392 を割り当てられました。

Cisco ASA Clientless SSL VPN 門脈カスタマイゼーション 統合脆弱性

Clientless SSL VPN 門脈カスタマイゼーション フレームワークの脆弱性は非認証が、リモート攻撃者信任状の窃盗を含む複数の不正侵入のクロスサイト スクリプティング（XSS）原因となる可能性があり、Web の他の型が影響を受けたシステムを使用しているクライアントで攻撃する Clientless SSL VPN ポータルの内容を修正するようにする可能性があります。

脆弱性は認証の不適当な実装が原因チェックインします Clientless SSL VPN 門脈カスタマイゼーション フレームワークをです。 攻撃者はいくつかの RAMFS キャッシュファイル システムの力

スタマイゼーション オブジェクトの修正によってこの脆弱性を不正利用する可能性があります。 エクスプロイトは攻撃者が Clientless SSL VPN 認証をバイパスし、門脈内容を修正することを可能にする可能性があります。

注: 本脆弱性を不正利用する目的で使用できるのは、該当システム宛てのトラフィックに限られます。 この脆弱性はルーティングされたファイアウォール モードと単一コンテキスト モードでだけ設定されるシステムだけ影響を及ぼします。 この脆弱性は IPv4 および IPv6 トラフィックによって引き起こすことができます。 有効な TCP ハンドシェイクがこの脆弱性を不正利用するために必要となります。

この脆弱性は Cisco バグ ID CSCup36829 （ 登録ユーザのみ ）で文書化されています、CVE ID CVE-2014-3393 を割り当てられました。

Cisco ASA Smart Call Home デジタル認証 検証脆弱性

Cisco ASA ソフトウェアの Smart Call Home （ SCH ）機能の脆弱性はデジタル証明書を使用するどの機能でも影響を受けたシステムで設定される場合リモート攻撃者非認証がデジタル認証 検証をバイパスするようにする可能性があります。

SCH が設定される時、トラストポイントが、Verisign 認証を含んで、自動的にインストールされているので存在 する脆弱性。 攻撃者は VeriSign によって署名した影響を受けたシステムへ有効な証明書を可能性があります示すことによって認証するときこの脆弱性を不正利用する。 不正利用はある特定の機能によって使用されたとき攻撃者が、たとえばデジタル認証認証をバイパスすることを可能にする、可能性があります。 デジタル証明書 検証を使用するために設定できる機能の例は VPN がおよび適応性がある安全 装置管理 (ASDM) 認証、TLS プロキシおよび電話プロキシ含まれています。

注: 本脆弱性を不正利用する目的で使用できるのは、該当システム宛てのトラフィックに限られます。 この脆弱性は単一およびマルチ コンテキスト モードのルーティングされたおよび透過ファイアウォール モード影響を与えます。 この脆弱性は IPv4 および IPv6 トラフィックによって引き起こすことができます。 有効な TCP ハンドシェイクがこの脆弱性を不正利用するために必要となります。

この脆弱性は Cisco バグ ID CSCun10916 （ 登録ユーザのみ ）で文書化されています、CVE ID CVE-2014-3394 を割り当てられました。

回避策

次の脆弱性に関しては影響を受けた機能をディセーブルにすることを除く回避策がありません:

- SQL*NET (Oracle) Cisco ASA インスペクション エンジン サービス拒否の脆弱性
- Cisco ASA VPN サービス拒否の脆弱性
- Cisco ASA IKEv2 サービス拒否の脆弱性
- Cisco ASA 健全性およびパフォーマンスモニタ サービス拒否の脆弱性

- Cisco ASA GPRS Tunneling Protocol（GTP）インスペクション エンジン サービス拒否の脆弱性
- Cisco ASA SunRPC インスペクション エンジン サービス拒否の脆弱性
- Cisco ASA DNS インスペクション エンジン サービス拒否の脆弱性
- Cisco ASA VNMC コマンド 入力 検証脆弱性
- Cisco ASA ローカル パス包含脆弱性
- Cisco ASA Clientless SSL VPN 情報の漏えいおよびサービス拒否の脆弱性
- Cisco ASA Clientless SSL VPN 門脈カスタマイゼーション 統合脆弱性
- Cisco ASA Smart Call Home デジタル認証 検証脆弱性

注: Cisco ASA Smart Call Home デジタル認証 検証脆弱性に関しては、SCH 設定を取除くことはトラストポイントを取除きません。 トラストポイントを除去するために、管理者は **crypto ca trustpoint <TP_name>** コマンドを使用する必要があります。 次の例に SCH 機能によってイネーブルになっているトラストポイントを取除く方法を示されています。 このトラストポイントを取除くにより SCH は正しくはたらくことを止めます。

```
ciscoasa(config)# no crypto ca trustpoint _SmartCallHome_ServerCA
```

Cisco ASA VPN Failover コマンド インジェクト脆弱性に関しては、Failover 鍵を設定することはこの問題に対応策を提供します。 Failover 鍵を設定するために、 **Failover 鍵 <key>** コマンドを使用して下さい。 次の例に Failover 鍵指名された *Cisco 鍵*を設定する方法を示されています:

```
ciscoasa(config)#failover key cisco-key
```

注: フェールオーバー ipsec コマンドの使用はこの問題に回避策を提供しません。

修正済みソフトウェア

ソフトウェアアップグレードを検討するとき、顧客は Cisco Security Advisory、応答および表記アーカイブを http://www.cisco.com/go/psirt で参照し、公開および完全なアップグレード ソリューションを判別するためにそれに続く状況報告を検討するように勧告されます。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。 不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンス プロバイダーにお問い合わせください。

Cisco 次の ASA ソフトウェア テーブルの各行は Cisco 各 ASA メジャーリリースのためのこの状況報告に説明がある脆弱性のそれぞれのための最初の修正済みリリースをリストします。 表の最後の行は Cisco 各 ASA メジャーリリースのためのこの状況報告に説明があるすべての脆弱性のための修正を含むリリースバージョンについての情報を与えます。 顧客はこれらのリリースバージョンよりまたはそれ以降と等しいリリースにアップグレードする必要があります。

	7.2	8.2	8.3
CSCum46027 - SQL*NET（Oracle） Cisco ASA	7.2(5.13)	8.2(5.50)	8.3(2.42)

インスペクション エンジン サービス拒否の脆弱性			
CSCul36176 - Cisco ASA VPN サービス拒否の脆弱性	Not affected	Not affected	Not affected
CSCum96401 - Cisco ASA IKEv2 サービス拒否の脆弱性	Not affected	Not affected	Not affected
CSCum00556 - Cisco ASA 健全性およびパフォーマンスモニタ サービス拒否の脆弱性	Not affected	Not affected	8.3(2.42)
CSCum56399 - Cisco ASA GPRS Tunneling Protocol（GTP）インスペクション エンジン サービス拒否の脆弱性	Not affected	8.2(5.51)	Not affected
CSCun11074 - Cisco ASA SunRPC インスペクション エンジン サービス拒否の脆弱性	7.2(5.14)	8.2(5.51)	8.3(2.42)
CSCuo68327 - Cisco ASA DNS インスペクション エンジン サービス拒否の脆弱性	Not affected	Not affected	Not affected
CSCuq28582 - Cisco ASA VPN Failover コマンド インジェクト脆弱性	7.2(5.15)	8.2(5.51)	8.3(2.42)
CSCuq41510 および CSCuq47574 - Cisco ASA VNMC コマンド 入力 検証脆弱性	Not affected	Not affected	Not affected
CSCtq52661 - Cisco ASA ローカル パス包含脆弱性	Not affected	8.2(5.52)	使用不可能- 8.4 またのアップグレード
CSCuq29136 - Cisco ASA Clientless SSL VPN 情報の漏えいおよびサービス拒否の脆弱性	Not affected	8.2(5.51)	8.3(2.42)
CSCup36829 - Cisco ASA Clientless SSL VPN 門脈カスタマイゼーション 統合脆弱性[3]	Not affected	8.2(5.51)[3]	8.3(2.42)[3]
CSCun10916 - Cisco ASA Smart Call Home デジタル認証 検証脆弱性	Not affected	8.2(5.50)	Not affected
この Security Advisory のすべての脆弱性を解決する推奨されるリリース	**7.2(5.15) およびそれ以降**	**8.2(5.52) およびそれ以降**	**使用不可能- 8.4 またのアップグレード**

[1]The Cisco ASA VPN サービス拒否の脆弱性は Cisco ASA ソフトウェア リリース 9.1(4.3) でもたらされました

[2]The Cisco ASA DNS インスペクション エンジン サービス拒否の脆弱性は Cisco ASA ソフトウェア リリース 9.0(4.8) および 9.1(5.2) でもたらされました。

[3]Customers は Cisco ASA Clientless SSL VPN 門脈カスタマイゼーション 統合脆弱性から影響を受ける方法でこの脆弱性を軽減するその他の情報のための「Cisco ASA Clientless SSL VPN 門脈カスタマイゼーション 統合脆弱性についての注記」セクションを読む必要があります。

注: Cisco ASA ソフトウェア リリース 9.3(1.1) は 2014 年 11月 10 日によって利用できます

Cisco ASA Clientless SSL VPN 門脈カスタマイゼーション 統合脆弱性についての注記

、ソフトウェア リリースに関係なく実行している顧客は脆弱な設定を門脈カスタマイゼーションが妥協されなかったことを確認する必要があります。 この脆弱性は更に不正利用されることを Cisco ASA ソフトウェアの修正済み バージョンへのアップグレードが防ぐ間、既にシステムに現在妥協され、であるカスタマイゼーション オブジェクトを修正しません。 攻撃者が既にカスタマイゼーション オブジェクトを妥協している場合、妥協されたオブジェクトはアップグレードの後で耐久性があるとどまります。

カスタマイゼーション オブジェクトが妥協されたかどうか確かめるために、「Cisco ASA Clientless SSL VPN 門脈カスタマイゼーション 統合脆弱性のための妥協の追加インジケータ」従って下さいこの状況報告の「脆弱性が存在する製品」セクションの手順にに含まれている。

次の方式がデフォルト カスタマイゼーション オブジェクト（ *DfltCustomization* ）を復元するのに使用することができます:

1. ファイルに既定のテンプレートをエクスポートして下さい。 次の例に *default_template* と呼ばれるファイルに既定のテンプレートをエクスポートする方法を示されています
2.
3. `ciscoasa# export webvpn customization Template default_template`
4.
5. デフォルト カスタマイゼーション オブジェクト（ *DfltCustomization* ）として既定のテンプレートをインポートして下さい:

```
ciscoasa# import webvpn customization DfltCustomization default_template
```

注: これはあったデフォルト カスタマイゼーション オブジェクト（ *DfltCustomization* ）への変更を無効にします。 システムからデフォルト カスタマイゼーション オブジェクト（ *DfltCustomization* ）を取除くことはできません。

インポート webvpn カスタマイゼーション コマンドも手動で編集され、確認されましたこれらの後でデフォルト以外のカスタマイゼーション オブジェクトを復元するのに使用することができます。 ASDM を使用し、 **CLIENTLESS SSL VPN アクセス**にナビゲートによってデフォルト以外のカスタマイゼーション オブジェクトを取除くことは可能性のある **- > PORTAL - > カスタマイゼーション**です。 カスタマイゼーション パネルで、デフォルト以外のカスタマイゼーション オブジェクトを選択し、『Delete』 をクリック して下さい。

ソフトウェアのダウンロード

Cisco ASA ソフトウェアは Cisco.com の Software Center から http://www.cisco.com/cisco/software/navigator.html の参照によってダウンロードすることができます

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスおよび Cisco ASA 5500-X 次世代ファイアウォールに関しては **製品 > Security > ファイアウォール > 適応型セキュリティ アプライアンス（ASA） > Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス > <your Cisco ASA model> に > 適応型セキュリティ アプライアンス（ASA）ソフトウェア（ASA）ソフトウェア** ナビゲートして下さい。 いくつかのこれらのバージョンが暫定バージョンで、Download ページことをの **暫時**タブの拡張によって見つけることができることに注目して下さい。

Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータの Cisco ASA サービス モジュールに関しては、 **製品 > Cisco インターフェイスおよびモジュール > Cisco サービス モジュール > Cisco Catalyst 6500 シリーズ/7600 シリーズ ASA サービス モジュール**に **> 適応型セキュリティ アプライアンス (ASA) ソフトウェア (ASA) ソフトウェア** ナビゲートして下さい。 いくつかのこれらのバージョンが暫定バージョンで、Download ページことをの **暫時**タブの拡張によって見つけることができることに注目して下さい。

Cisco ASA 1000V クラウド ファイアウォールに関しては、 **> 適応型セキュリティ アプライアンス (ASA) ソフトウェア (ASA) ソフトウェアは製品 > Security > ファイアウォール > 適応型セキュリティ アプライアンス (ASA) > Cisco ASA 1000V クラウド ファイアウォール**にナビゲート します。

のため Cisco 適応型セキュリティ仮想アプライアンス (ASAv) （ ASAv ）、 **製品 > Security > ファイアウォール > 適応型セキュリティ アプライアンス (ASA)** へのナビゲート **> Cisco 適応型セキュリティ仮想アプライアンス (ASAv) （ ASAv ） > 適応型セキュリティ アプライアンス (ASA) ソフトウェア (ASA) ソフトウェア。**

不正利用事例と公式発表

Cisco ASA VPN Failover コマンド インジェクト脆弱性、Cisco ASA VNMC コマンド 入力 検証脆弱性および Cisco ASA Clientless SSL VPN 門脈カスタマイゼーション統合脆弱性は Alec スチュワートMuirk によって Cisco に報告されました。

Cisco ASA VPN Failover コマンド インジェクト脆弱性の不正利用、Cisco ASA VNMC コマンド 入力 検証脆弱性、Cisco ASA Clientless SSL VPN 門脈カスタマイゼーション統合脆弱性および Cisco ASA ローカル パス包含脆弱性は Alec スチュワートMuirk によって Ruxcon 2014 セキュリティ会議で示されました。

Cisco ASA Clientless SSL VPN 情報の漏えいおよびサービス拒否の脆弱性は SecurityMetrics からの Hyrum M によって Cisco に報告されました。
この脆弱性のエクスプロイトを示す Hyrum M によるブログ ポストはまた共用利用可能です。

この状況報告に説明がある他のすべての脆弱性は内部テストまたはサポート ケースの解決の間に発見されました。

Cisco製品のセキュリティ上の問題に対する回答チーム (PSIRT) はこの状況報告に説明がある他の脆弱性に関するあらゆる公示に気づいていません。

Cisco PSIRT は Cisco ASA Clientless SSL VPN 門脈カスタマイゼーション 統合脆弱性の不正利用に気づいています。
顧客はこの Security Advisory の「Cisco ASA Clientless SSL VPN 「 ソフトウェア バージョン および 修正」セクションにの門脈カスタマイゼーション 統合脆弱性」についての注記目を通し、この脆弱性のための修正を含むバージョンにアップグレードするために助言しますあります

2015-July-08 アップデート: Cisco PSIRT は CVE-2014-3383 から影響を受ける Cisco ASA デバイスを持つ何人かの Cisco カスタマに中断にこの Security Advisory で表われた Cisco ASA VPN サービス拒否の脆弱性気づいています。 中断を引き起こすトラフィックにより特定のソース IPv4 アドレスに分離されました。 Cisco はトラフィックが悪意のある意図無しで送信 されたことをプロバイダおよびオーナーをそのデバイスのおよび判別される実行しました。 Cisco は remediate に Cisco 固定 ASA ソフトウェア リリースにことを顧客アップグレードこの問題強く推奨します。

Cisco PSIRT はこの状況報告に説明がある他の脆弱性の不正利用に気づいていません。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20141008-asa

改訂履歴

リビジョン 3.0	2015-July-09	Summary セクションの上に 7 月 8 日アップデート情報を移動しました。
リビジョン 3.0	2015-July-08	CSCul36176 のその他の情報を用いるこの状況報告の â Summaryâ および â 不正利用事例と公式発表」セクションを- Cisco ASA VPN サービス拒否の脆弱性アップデートしました。
Revision 2.0	2015-February-11	Cisco ASA Clientless SSL VPN 門脈カスタマイゼーション 統合脆弱性についての追加された重要な情報- CSCup36829 -この状況報告の「脆弱性が存在する製品」、「ソフトウェア バージョン および 修正」、および「不正利用事例と公式発表」セクションの…。
リビジョン 1.2	2015-January-13	CSCtq52661 のための最初修正済みリリースについての追加された情報。
リビジョン 1.1	2014-October-24	Cisco ASA ソフトウェア バージョン 9.3(1.1) および「不正利用事例と公式発表」セクションのための目標の期日をアップデートしました。
リビジョン 1.0	2014-October-08	初回公開リリース

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。 また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。