Cisco 適応型セキュリティ アプライアンス（ASA）の Web サービスにおける Denial of Service（DoS）の脆弱性

Critical

アドバイザリーID : cisco-sa-20180606-asaftd

初公開日 : 2018-06-06 16:00

最終更新日 : 2019-09-24 17:49

バージョン 1.4 : Final

CVSSスコア : 8.6

回避策 : No workarounds available

Cisco バグ ID : CSCvi16029

CVE-2018-0296

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

Cisco 適応型セキュリティ アプライアンス（ASA）の Web インターフェイスの脆弱性により、認証されていないリモートの攻撃者が該当デバイスの予期せぬリロードを引き起こし、結果として Denial of Service（DoS）状態となる場合があります。 特定のソフトウェア リリースでは ASA がリロードされない可能性もありますが、攻撃者はディレクトリ トラバーサル テクニックを利用することで、認証なしで機密のシステム情報を表示できる可能性があります。

この脆弱性は、HTTP URL の不完全な入力検証に起因します。 攻撃者は、該当デバイスに巧妙に細工された HTTP 要求を送信することにより、この脆弱性を不正利用する可能性があります。 不正利用により、攻撃者は DoS 状態を生じさせたり、認証されずに情報を開示させることができる場合があります。 この脆弱性は、IPv4 および IPv6 の両方の HTTP トラフィックに当てはまります。

シスコはこの脆弱性に対処するソフトウェア アップデートをリリースしました。 この脆弱性に対処する回避策はありません。

注: 継続的なエクスプロイトの試みがまん延しているため、この脆弱性が修正されている Cisco ASA ソフトウェア リリースにアップグレードすることを引き続き強くお勧めします。

このアドバイザリは、次のリンクより確認できます。
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-asaftd

該当製品

脆弱性のある製品

この脆弱性は、次のシスコ製品上で実行される Cisco ASA ソフトウェアおよび Cisco Firepower Threat Defense（FTD）ソフトウェアに影響を及ぼします。

- 3000 シリーズ産業用セキュリティ アプライアンス（ISA）
- ASA 1000V クラウド ファイアウォール
- 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製品群
- Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータ用の ASA サービス モジュール
- 適応型セキュリティ仮想アプライアンス（ASAv）
- FirePOWER 2100 シリーズ セキュリティ アプライアンス
- Firepower 4100 シリーズ セキュリティ アプライアンス
- FirePOWER 9300 ASA セキュリティ モジュール
- FTD Virtual（FTDv）

ASA ソフトウェア

次の表の左側の列に、脆弱な可能性のある Cisco ASA 機能を示します。 また右の列には、**show running-config** CLI コマンドで判断可能な、この機能の基本設定を示します。 デバイスにこれらの機能のいずれかが設定されている場合は、デバイスが脆弱かどうかの確認について追加の指示に従ってください。

Cisco ASA 機能	脆
Adaptive Security Device Manager（ASDM）[1]	ht ht <r <i
AnyConnect IKEv2 Remote Access（クライアント サービス有効時）	cr <i se w
AnyConnect IKEv2 Remote Access（クライアント サービス無効時）	cr <i w
AnyConnect SSL VPN	w <i
Cisco Security Manager [2]	ht ht <r <i

クライアントレス SSL VPN	w <i
カットスルー プロキシ（同じポートで他の脆弱な機能と組み合わせて使用していない限り脆弱性は存在しない）	aa <i <p
ローカル認証局（CA）	cr n
Mobile Device Manager（MDM）プロキシ[3]	m e
モバイル ユーザ セキュリティ（MUS）	w n <p n <p n <i
Proxy Bypass	w l
REST API[4]	re di re

[1]ASDM は、**http** コマンドで設定された範囲の IP アドレスに対してのみ脆弱です。
[2] Cisco Security Manager は、**http** コマンドで設定された範囲の IP アドレスに対してのみ脆弱です。
[3] MDM プロキシは、Cisco ASA ソフトウェア リリース 9.3.1 からサポートされています。
[4] REST API は、Cisco ASA ソフトウェア リリース 9.3.2 からサポートされています。 **http** コマンドで設定された範囲の IP アドレスに対してのみ脆弱です。

脆弱な可能性のある機能が設定されている ASA が脆弱かどうかについて確認する

ステップ 1： 管理者は、**show asp table socket | | include SSL||DTLS** コマンドを使用して、セキュア ソケット レイヤ（SSL）、または任意の TCP ポートの Datagram Transport Layer Security（DTLS）リッスン ソケットを探します。 コマンドの実行結果にどちらかのソケットが表示され、ASA デバイスで上記の表の ASA 機能が 1 つ以上設定されている場合、そのデバイスには脆弱性が存在すると考えられます。 次の例は、SSL と DTLS のリスニング ソケットが設定されている ASA デバイスを示しています。

```
ciscoasa# show asp table socket | include SSL|DTLS
```

```
ciscoasa# show asp table socket | include SSL|DTLS
```

ステップ 2 ： 管理者はさらに **show processes | include Unicorn** コマンドを使用して、脆弱性のあるプロセスがデバイスで実行されているかどうかを確認できます。 これは、脆弱な可能性のある機能のうちの 1 つによって内部 Web サーバのインスタンスが作成されたこと、つまり脆弱であることを意味します。 **Unicorn プロキシ スレッド**が存在している場合、そのデバイス

は脆弱であると考えられます。

```
ciscoasa# show processes | include Unicorn

Mwe 0x0000557f9f5bafc0 0x00007f62de5a90a8 0x0000557fa52b50a0        3632 0x00007f62c8c87030
30704/32768 Unicorn Proxy Thread 218
```

注: 上記例での *Unicorn プロキシ スレッド*識別子は *218* であり、これは変わる可能性があります。 実際のスレッド ID 番号に関係なく、 *Unicorn プロキシ スレッド*のプロセスが実行中の場合、デバイスは脆弱であるとみなされます。

実行している ASA ソフトウェア リリースの確認

デバイスで実行している Cisco ASA ソフトウェアが脆弱なリリースかどうかについては、管理者が CLI で **show version** | include Version コマンドを実行することで確認できます。 **| Include Version** コマンドを実行することで確認できます。 デバイスが Cisco ASA ソフトウェア リリース 9.2(1) を実行している場合は、コマンドの出力は次の例のようになります。

```
ciscoasa# show version | include Version

Cisco Adaptive Security Appliance Software Version 9.2(1)
Device Manager Version 7.4(1)
```

Cisco Adaptive Security Device Manager（ASDM）を使用してデバイスを管理している場合は、ログイン ウィンドウに表示される表、または Cisco ASDM ウィンドウの左上に、ソフトウェア リリースが表示されます。

FTD ソフトウェア

この脆弱性は、脆弱ではないリリース 6.2.0 を除き、すべての Cisco FTD ソフトウェア リリースに当てはまります。 Cisco FTD ソフトウェアの修正済みリリースについては、「 修正済みリリース」セクションを参照してください。 この Cisco FTD ソフトウェア リリースには、Firepower のコードと ASA のコードが両方含まれています。 詳細については、『 Cisco Firepower Compatibility Guide（Cisco Firepower 互換性ガイド）』の「Firepower Threat Defense Devices（Firepower Threat Defense デバイス）」を参照してください。

次の表の左側の列に、脆弱な可能性のある Cisco FTD 機能を示します。 また右の列には、**show running-config** CLI コマンドで判断可能な、この機能の基本設定を示します。 デバイスにこれらの機能のいずれかが設定されている場合は、デバイスが脆弱かどうかの確認について追加の指示に従ってください。

Cisco FTD 機能	脆弱性の存在するコンフィギュレーション
HTTP サービス有効 [1]	http server enable <port #> http <remote_ip_address> <remote_subnet_mask> <interface_name>
AnyConnect IKEv2 Remote Access（クライアント サービス有効時）[2、3]	crypto ikev2 enable <interface_name> client-services po #>

	webvpn anyconnect enable
AnyConnect IKEv2 Remote Access（クライアント サービス無効時）[2、3]	crypto ikev2 enable <interface_name> webvpn anyconnect enable
AnyConnect SSL VPN[2、3]	webvpn enable <interface_name>

[1] HTTP 機能は、Firepower Management Console（FMC）の **[Firepower Threat Defenseプラットフォーム設定（Firepower Threat Defense Platform Settings）] > [HTTP]** で有効にできます

[2] リモート アクセス VPN 機能は、Cisco FMC で **[デバイス（Devices）] > [VPN] > [リモートアクセス（Remote Access）]**、または、Cisco Firepower Device Manager（FDM）の **[デバイス（Devices）] > [リモートアクセスVPN（Remote Access VPN）]** で有効にできます。

[3] リモート アクセス VPN 機能は、Cisco FTD ソフトウェア リリース 6.2.2 からサポートされています。

脆弱な可能性のある機能が設定されている Cisco FTD が脆弱かどうかについて確認する

ステップ 1： 管理者は、**show asp table socket | | include SSL||DTLS** コマンドを使用して、TCP ポートの SSL または DTLS リスニング ソケットを検索することもできます。 コマンドの実行結果にどちらかのソケットが表示され、FTD デバイスで上記の表にリストされている機能の 1 つ以上が設定されている場合、そのデバイスには脆弱性が存在すると考えられます。次の例は、SSL と DTLS のリスニング ソケットが設定されている FTD デバイスを示しています。

```
firepower# show asp table socket | include SSL|DTLS

firepower# show asp table socket | include SSL|DTLS
```

ステップ 2 ： 管理者はさらに **show processes | include Unicorn** コマンドを使用して、脆弱性のあるプロセスがデバイスで実行されているかどうかを確認できます。 これは、脆弱な可能性のある機能のうちの 1 つによって内部 Web サーバのインスタンスが作成されたこと、つまり脆弱であることを意味します。 **Unicorn プロキシ スレッド**が存在している場合、そのデバイスは脆弱であると考えられます。

```
firepower# show processes | include Unicorn

Mwe 0x0000557f9f5bafc0 0x00007f62de5a90a8 0x0000557fa52b50a0       3632 0x00007f62c8c87030
30704/32768 Unicorn Proxy Thread 218
```

注：

- 上記例での *Unicorn プロキシ スレッド*識別子は *218* であり、これは変わる可能性があります。 実際のスレッド ID 番号に関係なく、*Unicorn プロキシ スレッド*のプロセスが実行中の場合、デバイスは脆弱であるとみなされます。
- IKEv2 の特定の機能セットでは、ベースの SSL TCP リスニング ソケットが有効になって

いなくても脆弱性が存在する可能性があります。 管理者は **show running-config crypto ikev2** CLI コマンドを使用して、下記例のように **crypto ikev2 enable** コンフィギュレーション コマンドが設定に存在しているかどうかを確認できます。

```
firepower# show running-config crypto ikev2 | include enable

crypto ikev2 enable Outside
```

実行コンフィギュレーションに **crypto ikev2 enable** コマンドが設定されており、**anyconnect enable** コマンドがグローバル **webvpn** コンフィギュレーションに含まれている場合、その Cisco FTD デバイスにも脆弱性が存在すると考えられます。

実行している Cisco FTD ソフトウェア リリースの確認

管理者は CLI から **show version** コマンドを使用することにより、Cisco FTD リリースを確認できます。 デバイスでリリース 6.2.2 が実行されている場合、次の例のようになります。

```
> show version

--------------------[ ftd ]---------------------
Model : Cisco ASA5525-X Threat Defense (75) Version 6.2.2 (Build 362)
UUID : 2849ba3c-ecb8-11e6-98ca-b9fc2975893c
Rules update version : 2017-03-15-001-vrt
VDB version : 279
-------------------------------------------------
```

脆弱性を含んでいないことが確認された製品

このアドバイザリの脆弱性が存在する製品のセクションにリストされている製品だけ既知この脆弱性によって影響されるためにである。

シスコは、Cisco AnyConnect セキュア モビリティ クライアントには脆弱性が存在しないことを確認済みです。

回避策

この脆弱性に対処する回避策はありません。

修正済みソフトウェア

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェア アップデートを提供しています。 お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。 そのようなソフトウェア アップグレードをインストール、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、お客様は以下のリンクに記載されたシスコのソフトウェア ライセンスの条項に従うことに同意したことになります。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。 通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。 無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

ソフトウェアのアップグレードを検討する際には、Cisco Security Advisories and Alerts ページで入手できるシスコ製品のアドバイザリを定期的に参照して、侵害を受ける可能性と完全なアップグレード ソリューションを確認してください。

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は新規リリースでも継続して適切なサポートが受けられることを確認してください。 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。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティ ベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC に連絡してアップグレードを入手してください。
https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

修正済みリリース

次の表に示すように、適切なリリースにアップグレードする必要があります。

Cisco ASA ソフトウェア

Cisco ASA ソフトウェア リリース	この脆弱性に対する最初の修正リリース
9.1[1] 前	9.1.7.29 への移行が必要
9.1	9.1.7.29
9.2	9.2.4.33
9.3[1]	9.4.4.18 への移行が必要
9.4	9.4.4.18
9.5[1]	9.6.4.8 への移行が必要
9.6	9.6.4.8
9.7	9.7.1.24
9.8	9.8.2.28
9.9	9.9.2.1

[1] Cisco ASA ソフトウェアの 9.1 より前のリリース、Cisco ASA リリース 9.3、および 9.5 については、ソフトウェア メンテナンスが終了しています。 お客様は、サポートされているリリースに移行する必要があります。

ソフトウェアは、Cisco.com の Software Center で、[製品（Products）] > [セキュリティ（Security）] > [ファイアウォール（Firewalls）] > [適応型セキュリティアプライアンス（ASA）（Adaptive Security Appliances (ASA)）] > [ASA 5500-Xシリーズファイアウォール（ASA 5500-X Series Firewalls）] の順に選択すると ASA ハードウェア プラットフォームのリストが表示されるので、そこからダウンロードできます。 これらのソフトウェア リリースの大半は、暫定版として表示されます。

Cisco FTD ソフトウェア

Cisco FTD ソフトウェア リリース	この脆弱性に対する最初の修正リリース
6.0	6.1.0 ホットフィックス以降への移行が必要
6.0.1	6.1.0 ホットフィックス以降への移行が必要
6.1.0	Cisco_FTD_Hotfix_EI-6.1.0.7-2.sh（41*xx* および 9300 を除く全 FTD ハードウェア プラットフォーム用） Cisco_FTD_SSP_Hotfix_EI-6.1.0.7-2.sh（41*xx* および 9300 FTD ハードウェア プラットフォーム用）
6.2.0	脆弱性なし
6.2.1	6.2.2.3 への移行が必要
6.2.2	6.2.2.3
6.2.3	6.2.3.1 6.2.3-85[1] 6.2.3-85.0[2]

[1] Microsoft Azure クラウド用の FTD Virtual のソフトウェア イメージ
[2] AWS クラウド用の FTD Virtual のソフトウェア イメージ

ソフトウェアは、Cisco.com の Software Center で、[製品（Products）] > [セキュリティ（Security）] > [ファイアウォール（Firewalls）] > [次世代ファイアウォール（NGFW）（Next-Generation Firewalls (NGFW)）] の順に選択すると、利用可能な FTD ハードウェア プラットフォームのリストが表示されるので、そこからダウンロードできます。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）は、2019 年 9 月に、この脆弱性のさらなるエクスプロイトが試みられたことを認識しました。 この脆弱性が修正されている Cisco ASA ソフトウェア リリースにアップグレードすることを、引き続き強くお勧めします。

出典

シスコは、この脆弱性の発見と報告をしていただいたセキュリティ研究者 Michal Bentkowski 氏に感謝いたします。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-asaftd

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.4	SIR 値を Critical に変更、サマリーへのアップグレードに関する注記を追加、エクスプロイトと公式発表のセクション中のエクスプロイト情報を更新。	SIR、サマリ、不正利用事例と公式発表	最終版	2019年9月24日
1.3	「エクスプロイト事例と正式発表」の項のエクスプロイトに関する情報を更新。	不正利用事例と公式発表	最終版	2019年3月6日
1.2	影響を受けないバージョン 6.2.0 を削除するためにアドバイザリ メタデータを修正。		最終版	2018年10月5日
1.1		不正利用事例と公式発表	最終版	2018年6月2

				2日
1.0	初回公開リリース		最終版	2018年6月6日

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。