Cisco Web セキュリティ アプライアンスにおける FTP 認証バイパスの脆弱性

High

アドバイザリーID : cisco-sa-20180307-wsa

初公開日 : 2018-03-07 16:00

バージョン 1.0 : Final

CVSSスコア : 7.3

回避策 : No workarounds available

Cisco バグ ID : CSCvf74281

CVE-2018-0087

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 Web セキュリティ アプライアンス (WSA) の FTP サーバにおける脆弱性により、未認証のリモート攻撃者が、有効なパスワードを指定せずにデバイスの FTP サーバに口グインできる可能性があります。 ただし、有効なユーザ名が必要です。

この脆弱性は、FTP でユーザ クレデンシャルが正しく確認されないことに起因しており、 標的となったデバイスの管理 IP アドレスに FTP 接続されることで、不正利用される可能性があります。 不正利用されると、攻撃者が有効なパスワードを指定せずに Cisco WSA の FTP サーバに口グインできるようになる可能性があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。この脆弱性に対処する回避策はありません。

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-20180307-wsa

該当製品

脆弱性のある製品

この脆弱性は、仮想アプライアンスおよびハードウェア アプライアンス上で実行されている、WSA ソフトウェア用 Cisco AsyncOS 10.5.1 のいずれかのリリースに影響します。 影響を受けるソフトウェア リリースの詳細については、本セキュリティ アドバイザリの「修正済みソフトウェア」セクションを参照してください。

デバイスに脆弱性が生じるのは、管理インターフェイスで FTP が有効になっている場合のみです。 FTP はデフォルトでは無効になっています。

FTP 設定状況の確認

管理インターフェイスの FTP 設定状況を確認するには、管理者権限で、次の 3 つのうちいずれかの方法を実施します。

FTP 設定状況を確認するための第 1 の方法

管理者は、**showconfig** コマンドを実行することで、管理インターフェイスの *ftpd* ポートの設定状況をチェックできます。

```
ciscowsa> showconfig
Choose the password option:
1. Mask passwords (Files with masked passwords cannot be loaded using loadconfig command)
2. Plain passphrases
[1]> 1
.
.
.
<interfaces>
<interface>
<interface_name>Management</interface_name>
<ip>x.x.x.x</ip>
<phys_interface>Management</phys_interface>
<netmask>24</netmask>
<interface_hostname>xxx.xxx.xxx</interface_hostname>
<ftpd_port>21</ftpd_port>
.
.
.
```

FTP 設定状況を確認するための第 2 の方法

管理者は、**ifconfig** コマンドを実行することで、FTP 設定状況をチェックできます。 下記の例では、管理インターフェイスで FTP が設定されていることがわかります。 角かっこ内の *Y* 値が現在の設定を表しています。

```
ciscowsa> ifconfig
.
.
.
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
- DETAILS - Show details of an interface.
>EDIT

Enter the number of the interface you wish to edit.
[]> 1
.
```

```
.
Do you want to enable FTP on this interface? [Y]>
.
.
.
```

FTP 設定状況を確認するための第 3 の方法

管理者は、GUI を使用して FTP 設定状況をチェックすることもできます。[ネットワーク（Network）] > [インターフェイス（Interfaces）] > [アプライアンス管理サービス（Appliance Management Services）] の順に移動して、[FTP] チェック ボックスが選択されているか確認します。

WSA ソフトウェア リリースの確認

脆弱性のある Cisco AsyncOS ソフトウェア リリースが Cisco WSA で実行されているかどうかは、管理者が WSA CLI で **version** コマンドを使用することで確認できます。 Cisco ASyncOS ソフトウェア リリース 10.5.1-296 を実行しているアプライアンスでの出力例を以下に示します。

```
ciscowsa> version
Current Version
===============
Product: Cisco IronPort S670 Web Security Appliance
Model: S670
Version: 10.5.1-296
.
.
.
```

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。

次の製品は、この脆弱性の影響を受けません。

- E メール セキュリティ アプライアンス（ESA）の仮想バージョンとハードウェア バージョンの両方
- Security Mail Appliance（SMA）の仮想バージョンとハードウェア バージョンの両方

回避策

この脆弱性に対処する回避策はありません。 ただし、この脆弱性が存在するのは、管理インターフェイスで FTP が有効になっている場合のみです。 FTP が無効になっている場合は存在しません。 したがって、FTP を無効にすることが、この脆弱性の回避策となります。

管理インターフェイスの FTP を無効にする

管理インターフェイスの FTP を無効にするには、管理者権限で、次の 2 つのうちいずれかの方法

を実施します。

管理インターフェイスの FTP を無効にするための第 1 の方法

管理者は、**ifconfig** コマンドを実行して管理インターフェイスの設定を編集した後、**commit** コマンドを実行して変更を確定することで、FTP を無効にすることができます。

```
ciscowsa> ifconfig
.
.
.
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
- DETAILS - Show details of an interface.
>EDIT

Enter the number of the interface you wish to edit.
[]> 1
.
.
Do you want to enable FTP on this interface? [Y]> N
.
.
.
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
- DETAILS - Show details of an interface.
[]>
ciscowsa> commit
Warning: In order to process these changes, the proxy process will restart after Commit. This
will cause a brief interruption in service. Additionally, the authentication cache will be
cleared, which might require some users to authenticate again.

Warning: Processing of network configuration changes might cause a brief interruption in network
availability.

Please enter some comments describing your changes:
[]> disable FTP

Changes committed
.
.
.
```

管理インターフェイスの FTP を無効にするための第 2 の方法

管理者は、GUI から FTP を無効にすることができます。[ネットワーク（Network）] > [インターフェイス（Interfaces）] > [アプライアンス管理サービス（Appliance Management Services）] の順に移動し、[FTP] チェック ボックスの選択を解除してから、[送信（Submit）] をクリックして変更を確定します。

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。
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.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。

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。
http://www.cisco.com/en/US/support/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

次の表では、左の列に、WSA ソフトウェア用 Cisco AsyncOS のメジャー リリースを示しています。 右の列は、メジャー リリースが本アドバイザリに記載している脆弱性に該当するかどうか、また、本脆弱性に対する修正を含む最初のマイナー リリースに該当するかどうかを示します。

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。

WSA ソフトウェア用 Cisco	このアドバイザリに対する最初の修正リリース

AsyncOS のメジャー リリース	
10.5.1 よりも前	脆弱性なし
10.5.1	10.5.2-042 以降
11.0 以降	脆弱性なし

WSA の更新は、ほとんどの場合、システム管理 GUI の [システムアップグレード（System Upgrade）] オプションを使用することにより、ネットワーク経由で実行できます。 システム管理 GUI を使用してデバイスをアップグレードするには、管理者権限で次の手順を実施します。

1. [システム管理（System Administration）] > [システムアップグレード（System Upgrade）] を選択します。
2. [アップグレード（Upgrade）] オプションをクリックします。
3. [ダウンロードしてインストール（Download and Install）] を選択します。
4. アップグレードするリリースを選択します。
5. [アップグレード準備（Upgrade Preparation）] 領域で、適切なオプションを選択します。
6. [続行（Proceed）] をクリックすると、アップグレードが始まります。 アップグレードのステータスを示す経過表示バーが表示されます。

アップグレードが完了すると、デバイスがリブートします。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例やその公表を確認していません。

出典

本脆弱性は、シスコ TAC のサポート案件の対応時に発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180307-wsa

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2018 年 3 月 7 日

利用規約

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。