Cisco Web Security Appliance Web Proxy Memory Exhaustion Denial of Service Vulnerability

High

アドバイザリーID : cisco-sa-20180815-wsa-dos

初公開日 : 2018-08-15 16:00

バージョン 1.0 : Final

CVSSスコア : 8.6

回避策 : No workarounds available

Cisco バグ ID : CSCvf36610

CVE-2018-0410

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 AsyncOS Software for Cisco Web Security Appliances の Web プロキシの脆弱性により、未認証のリモートの攻撃者がシステム メモリを使い果たし、対象システムのサービス妨害（Dos）状態を引き起こします。

この脆弱性は、影響を受けるソフトウェアによる対象デバイスへの TCP 接続のメモリ リソース管理が不適切なことが原因で発生します。 攻撃者は、IPv4 または Ipv6 経由で影響を受けるデバイスのデータ インターフェイスに対して非常に多くの TCP 接続を確立することにより、この脆弱性を不正利用する可能性があります。 この不正利用が成功した場合、攻撃者はシステム メモリを使い果たす可能性があり、それによって、システムは新しい接続の処理を停止し、結果的に DoS 状態になります。 システム リカバリには、手動による介入が必要な場合があります。

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-20180815-wsa-dos
[英語]

該当製品

脆弱性のある製品

この脆弱性は、HTTPS Proxy 機能が有効な場合、仮想およびハードウェア アプライアンスの両方で Cisco Web Security Appliances の Cisco AsyncOS ソフトウェア リリース 9.1、10.1、10.5、および 11.0 に影響があります。 デフォルトでは、HTTPS Proxy 機能はディセーブルになっています。

脆弱性が存在する Cisco AsyncOS ソフトウェア リリースについては、このアドバイザリの「修正済みソフトウェア」セクションを参照してください。

脆弱性のある Cisco AsyncOS ソフトウェア リリースが Cisco Web Security Appliance (WSA) で実行されているかどうかは、管理者が WSA CLI で **version** コマンドを使用して確認できます。 デバイスが Cisco ASA ソフトウェア リリース 10.5.2-072 を実行している場合、WSA のコマンドの出力例は次のようになります。

```
ciscowsa> version

Current Version
===============
Product: Cisco S670 Web Security Appliance
Model: S670
Version: 10.5.2-072
.
.
.
```

WSA で HTPPS Proxy 機能がイネーブルかどうかは、管理者が WSA のWeb インターフェイスにログインし、 **セキュリティ サービス > HTTPS プロキシ** から確認できます。 **HTTPS プロキシ** フィールドの値は、機能を有効または無効にするかどうかを示します。

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のある製品セクションに記載されている製品のみが、この脆弱性の影響を受けることが分かっています。

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- 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 アプライアンスの両方
- 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

セキュリティ侵害の痕跡

脆弱性を悪用することで、ソフトウェアは確立した TCP 接続 に割り当てられたメモリ リソースの解放を停止し、それによって、当該デバイスのシステム メモリが使い果たされる可能性があります。

管理者は、デバイス CLI で **netstat コマンド** を使用することでデバイス接続の現在のステータスを評価できます。 コマンドの出力で *CLOSE_WAIT* 状態の TCP 接続の累積が示される場合、当

該デバイスは脆弱性の影響を受けている可能性があります。 次の例では、 IPv4 と IPv6 ので動作している複数のTCP接続でメモリ リソースが解放されていないデバイスに対して、 **netstat コマンド** の出力を示しています。

```
ciscowsa> netstat

.
.
.
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        (state)
tcp4       0      0 127.0.0.1.25255        127.0.0.1.36586        TIME_WAIT
tcp4   112    0 127.0.0.1.443      127.0.0.1.9310     CLOSE_WAIT
tcp4       0      0 127.0.0.1.9310         127.0.0.1.443          FIN_WAIT_2
tcp4       0      0 127.0.0.1.25255        127.0.0.1.21834        TIME_WAIT
tcp4   112    0 127.0.0.1.443      127.0.0.1.36782     CLOSE_WAIT
tcp4       0      0 10.1.1.51.32969     1.1.1.1.443        ESTABLISHED
tcp6   112    0 ::1.443          ::1.48808        CLOSE_WAIT
tcp4       0      0 10.1.1.51.443        *.*                    LISTEN
tcp6       0      0 ::1.443                 *.*                    LISTEN
tcp4       0      0 127.0.0.1.443          *.*                    LISTEN
.
.
.
```

デバイスのメモリ リソースを回復するには、管理者は、デバイスをリブートするか、またはWebプロキシのプロセスを再起動することができます。 Web プロキシ プロセスを再起動するには、管理者は、例えば、非表示の **診断 > プロキシ > kick** コマンドをなどを使用できます。

```
ciscowsa> diagnostic

Choose the operation you want to perform:
- NET - Network Diagnostic Utility.
- PROXY - Proxy Debugging Utility.
- REPORTING - Reporting Utilities.
[]> proxy

- SNAP    - Take a snapshot of the proxy
- OFFLINE - Take the proxy offline (via WCCP)
- RESUME  - Resume proxy traffic via (via WCCP)
- CACHE   - Clear proxy cache
[]> kick
Kick the proxy?
Are you sure you want to proceed? [N]> Y
```

Web プロキシ プロセスの再起動中に、その Web プロキシ サービスは一時的に使用できないことにに注意してください。

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。
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ことをお勧めします。

Cisco AsyncOS ソフトウェア メジャー リリース	First Fixed Release (修正された最初のリリース)
9.1	10.1.3-054以降に移行
9.1	10.1.3-054以降に移行
10.1	10.1.3-054
10.5	10.5.2-072
11.0	11.5.0-614

11.5	脆弱性なし

ソフトウェアのアップグレードは、ほとんどの場合、WSA の Web インターフェイスシステムの [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。 Web インターフェイスを使用してデバイスをアップグレードする場合

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、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180815-wsa-dos

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2018 年 8 月 15 日

利用規約