Cisco Wide Area Application Services Remote Code Execution Vulnerability

Advisory ID: cisco-sa-20140521-waas

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140521-waas

Revision 1.0

For Public Release 2014 May 21 16:00 UTC (GMT)

目次

要約

Cisco Wide Area Application Services（WAAS）ソフトウェア バージョン 5.1.1 ～ 5.1.1d には脆弱性が存在します。SharePoint アクセラレーション機能を設定している場合、認証されていないリモートの攻撃者がバッファ オーバーフローを不正利用して任意のコードを実行できるようになる可能性があります。

この脆弱性は、SharePoint の応答に対する不適切なバッファ処理に起因しています。攻撃者は、ユーザを悪意ある SharePoint アプリケーションにアクセスするように仕向けることで、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者はアプリケーション最適化ハンドラをクラッシュさせるとともに、WAAS アプライアンスに対する権限の昇格により任意のコードを実行できるようになります。

シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。このアドバイザリは、次のリンクで確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140521-waas

該当製品

脆弱性が認められる製品

次の製品は、脆弱性のある Cisco WAAS ソフトウェア バージョンが稼働し、SharePoint プリフェッチ オプションが設定されている場合に、この脆弱性の影響を受けます。

- Cisco WAAS アプライアンス
- Cisco Virtual WAAS（vWAAS）
- Cisco WAAS モジュール

プリフェッチ オプションは、 **accelerator http sharepoint-opt prefetch enable** コマンドで有効になります。このオプションは、デフォルトで無効です。

注：この脆弱性の影響を受けるのは、Cisco WAAS ソフトウェア リリース 5.1.1 ～ 5.1.1.d までです。

SharePoint プリフェッチ オプションが有効になっているかどうかは、次のいずれかの方法で判断できます。

sh run | include prefetch の出力を確認します。このコマンドが次の例のような出力を返す場合は、プリフェッチ オプションが有効になっています。

```
waas_lab#sh run | include prefetch
accelerator http sharepoint-opt prefetch enable
```

show accelerator http コマンドの出力で、 **SharePoint Prefetch** 行を探します。次の出力例は、SharePoint アクセラレータがシステムで有効になっていることを示しています。

```
waas_lab#show accelerator http

Accelerator    Licensed       Config State   Operational State
-----------    --------       ------------   -----------------
http           Yes            Enabled        Running

HTTP:
   Accelerator Config Item            Mode        Value
   -----------------------            ----        ------
   Suppress Server Encoding           Default     Disabled
[...]
   Sharepoint Prefetch                User        Enabled
[...]
```

脆弱性が認められない製品

次の製品は、Cisco WAAS ソフトウェアが稼働していても、この脆弱性の影響を受けません。

- Cisco WAAS Express（WAASx）
- Cisco WAAS Mobile

他のシスコ製品において、この脆弱性の影響を受けるものは現在確認されていません。

詳細

Cisco WAAS アプリケーション アクセラレーションおよび WAN 最適化ソリューションは、WAN を通じて提供される TCP ベースのアプリケーションのパフォーマンスを高めることで、ブランチ オフィスのデータ統合や中央集中型アプリケーションの高速化に効果をもたらします。

Cisco WAAS の SharePoint プリフェッチ最適化コードには脆弱性があるため、認証されていないリモートの攻撃者が最適化プロセスをクラッシュさせ、該当システムで任意のコードを実行できるようになる可能性があります。

この脆弱性は、特定タイプの要求を適切に検証できないことに起因します。攻撃者は、該当デバイスが最適化するユーザ要求に対して無効な形式の応答を提供する不正な SharePoint インストール環境に、ユーザが接続するよう仕向けることで、この脆弱性を不正利用する可能性があります。攻撃に成功すると、攻撃者は権限昇格によってデバイスに対し任意のコードを実行できるようになります。

注：この脆弱性の影響を受けるのは、SharePoint プリフェッチ最適化が設定されている Cisco WAAS ソフトウェアだけです。このオプションは、デフォルトで無効です。

この脆弱性は、Cisco Bug ID CSCue18479（ 登録ユーザ専用 ）として文書化され、Common Vulnerabilities and Exposures（CVE）ID CVE-2014-2196 が割り当てられています。

脆弱性スコア詳細

シスコは本アドバイザリでの脆弱性に対し、Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。本セキュリティ アドバイザリでの CVSS スコアは、CVSS バージョン 2.0 に基づいています。

CVSS は、脆弱性の重要度を示唆するもので、緊急性および対応の優先度を決定する組織の手助けとなる標準ベースの評価法です。

シスコでは、基本評価スコア（Base Score）および現状評価スコア（Temporal Score）を提供しています。お客様はこれらを用いて環境評価スコア（Environmental Score）を算出し、自身のネットワークにおける脆弱性の影響度を知ることができます。

シスコは次のリンクで CVSS に関する追加情報を提供しています。
http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

またシスコでは、各ネットワークにおける環境影響度を算出する CVSS 計算ツールを次のリンクで提供しています。
http://tools.cisco.com/security/center/cvssCalculator.x

CSCue18479 - WAAS / remote code execution vulnerability in httpmuxd Calculate the environmental score of					
CVSS Base Score - **9.3**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	None	Complete	Complete	Complete
CVSS Temporal Score - **7.7**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

この脆弱性の不正利用に成功すると、攻撃者は権限を昇格させ、該当システムに対して任意のコ

ードを実行できるようになる可能性があります。

ソフトウェア バージョンおよび修正

次の表は、Cisco WAAS ソフトウェアのメジャー リリースごとに推奨リリースを示したものです。

Major Releases	Recommended Release
4.x	Not affected
5.0.x	Not affected
5.1.x	5.1.1e
5.2.x	Not affected
5.3.x	Not affected

注：この脆弱性の影響を受けるのは、Cisco WAAS ソフトウェア リリース 5.1.1 ～ 5.1.1.d までです。

ソフトウェアのアップグレードを検討する場合は、 http://www.cisco.com/go/psirt/ の Cisco Security Advisories, Responses, and Notices アーカイブや、後続のアドバイザリを参照して、起こりうる障害を判断し、それに対応できるアップグレード 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、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。

回避策

この脆弱性を軽減する回避策はありません。

修正済みソフトウェアの入手

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。ソフトウェアの導入を行う前に、お客様のメンテナンス プロバイダーにご相談いただくか、ソフトウェアのフィーチャ セットの互換性およびお客様のネットワーク環境の特有の問題をご確認ください。

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、ご購入いただいたフィーチャ 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、アクセスまたはその他の方法で使用した場合、お客様は http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html に記載の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。

サービス契約をご利用のお客様

サービス契約をご利用のお客様は、通常のアップデート チャネルからアップグレード ソフトウェアを入手してください。ほとんどのお客様は、 Cisco.com の Software Navigator からアップグレードを入手することができます。 http://www.cisco.com/cisco/software/navigator.html

サードパーティのサポート会社をご利用のお客様

シスコ パートナー、正規販売代理店、サービス プロバイダーなど、サードパーティのサポート会

社と以前に契約していたか、または現在契約しており、その会社からシスコ製品の提供または保守を受けているお客様は、該当するサポート会社に連絡し、正しい処置についてのサポートを受けてください。

回避策や修正の効果は、使用している製品、ネットワーク トポロジー、トラフィックの性質や組織の目的などに関するお客様の状況によって異なります。影響を受ける製品やリリースは多種多様であるため、回避策を実施する前に、対象ネットワークで適用する回避策または修正が最適であることを、お客様のサービス プロバイダーやサポート会社にご確認ください。

サービス契約をご利用でないお客様

シスコから製品を直接購入したもののシスコのサービス契約をご利用いただいていない場合、または、サードパーティ ベンダーから購入したものの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 Technical Assistance Center（TAC）に連絡してアップグレード ソフトウェアを入手してください。

- +1 800 553 2447（北米からの無料通話）
- +1 408 526 7209（北米以外からの有料通話）
- Eメール：tac@cisco.com

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。サービス契約をご利用でないお客様は TAC に無償アップグレードをリクエストしてください。

さまざまな言語向けの各地の電話番号、説明、電子メール アドレスなどの、この他の TAC の連絡先情報については、シスコ ワールドワイドお問い合わせ先（http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html）を参照してください。

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不正利用事例とその公表は確認しておりません。

この通知のステータス：FINAL

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を示唆するものでもありません。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。またシスコはいつでも本ドキュメントの変更や更新を実施する権利を有します。

後述する情報配信の URL を省略し、本アドバイザリの記述内容に関して単独の転載や意訳を実施した場合には、事実誤認ないし重要な情報の欠落を含む統制不可能な情報の伝搬が行われる可能性があります。

情報配信

このアドバイザリは次のリンクにある Cisco Security Intelligence Operations に掲載されます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140521-waas

また、このアドバイザリのテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで次の電子メールで配信されています。

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk

本アドバイザリに関する今後の更新は Cisco.com に掲載されますが、メーリング リストで配信されるとは限りません。更新内容については、本アドバイザリの URL でご確認ください。

更新履歴

Revision 1.0	2014-May-21	Initial public release.

シスコ セキュリティ手順

シスコ製品におけるセキュリティの脆弱性の報告、セキュリティ事故に関するサポート、およびシスコからセキュリティ情報を入手するための登録方法の詳細については、Cisco.com の http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html を参照してください。この Web ページには、シスコのセキュリティ アドバイザリに関してメディアが問い合わせる際の指示が掲載されています。すべてのシスコ セキュリティ アドバイザリは、http://www.cisco.com/go/psirt/ で確認することができます。