Cisco Wide Area Application Servicesのリモートコード実行の脆弱性

アドバイザリーID : cisco-sa-20140521-waas
初公開日 : 2014-05-21 16:00
バージョン 1.0 : Final
CVSSスコア : 9.3
回避策 : No Workarounds available
Cisco バグ ID : CSCue18479

CVE-2014-2196

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 Wide Area Application Services(WAAS)ソフトウェアバージョン5.1.1 ~ 5.1.1dの脆弱性は、SharePointアクセラレーション機能で設定されている場合、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す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ます。攻撃者は、悪意のあるSharePointアプリケーションにアクセスするようユーザを誘導することで、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、WAASアプライアンスで権限を昇格させた上で任意のコードを実行する可能性があります。

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ています。このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140521-waas

該当製品

脆弱性のある製品

脆弱性のあるバージョンのCisco WAASソフトウェアを実行し、SharePointプリフェッチオプションが設定されている次の製品は、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になっています。

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のみです。

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を確認するには、次のいずれかの操作を行います。

sh runの出力を確認します。 | include prefetchコマンドを使用します。コマンドが次の例のように戻った場合は、プリフェッチオプションが有効になっています。
<#root>

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

show accelerator httpコマンドの出力を調べて、 SharePoint Prefetch行を探します。次の出力例は、SharePointアクセラレータを有効にしたシステムを示しています。
<#root>

```
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
[...]
```

脆弱性を含んでいないことが確認された製品

Cisco WAASソフトウェアを実行している次の製品は、この脆弱性の影響を受けません。

- Cisco WAAS Express(WAASx)
- Cisco WAASモバイル

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 WAASアプリケーションの高速化およびWAN最適化ソリューションは、WAN経由で配信されるTCPベースのアプリケーションのパフォーマンスを高速化し、ブランチオフィスのデータ統合と一元化されたアプリケーションの高速化というメリットを提供します。

Cisco WAASのSharePointプリフェッチ最適化コードにおける脆弱性により、認証されていないリモートの攻撃者が最適化プロセスのクラッシュを引き起こし、該当システムで任意の実行コードが実行される可能性があります。

この脆弱性は、特定の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、該当デバイスによって最適化されるユーザ要求に対して不正な応答を提供する可能性がある悪意のあるSharePointインストールにユーザを接続させることで、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、攻撃者は昇格された特権を使用してデバイス上で任意のコードを実行できる可能性があります。

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たCisco WAASソフトウェアのみです。このオプションはデフォルトで無効になっています。

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 Exposure(CVE)IDとしてCVE-2014-2196が割り当てられています。

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

次の表に、各Cisco WAASソフトウェアメジャーリリースの推奨リリースを示します。

メジャー リリース	推奨リリース
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のみです。

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 のシスコ セキュリティ アドバイザリ、応答、および通知のアーカイブや、後続のアドバイザリを参照して侵害の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。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）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やその公表を確認していません。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140521-waas

改訂履歴

リビジョン 1.0	2014年5月21日	初回公開リリース

利用規約

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。