CiscoワイヤレスLANコントローラのHTTP解析におけるDoS脆弱性

アドバイザリーID : cisco-sa-20160420-htrd CVE-2016-1363
初公開日 : 2016-04-20 16:00
バージョン 1.0 : Final
CVSSスコア : 10.0
回避策 : No workarounds available
Cisco バグ ID : CSCus25617

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 Wireless LAN Controller(WLC)ソフトウェアのHTTP URLリダイレクト機能の脆弱性により、認証されていないリモートの攻撃者が該当デバイスでバッファオーバーフロー状態を引き起こし、その結果サービス妨害(DoS)状態が発生する可能性があります。

この脆弱性は、該当ソフトウェアによるHTTPトラフィックの不適切な処理に起因します。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。エクスプロイトに成功すると、デバイスのバッファオーバーフロー状態が引き起こされ、デバイスのリロードが引き起こされてDoS状態が発生したり、デバイスで任意のコードが実行されたり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で確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160420-htrd

該当製品

脆弱性のある製品

Cisco WLCソフトウェアの次のリリースには脆弱性が存在します。

- すべての7.2リリース
- すべての7.3リリース

- 7.4.140.0(MD)より前のすべての7.4リリース
- すべての7.5リリース
- すべての7.6リリース
- 8.0.115.0(ED)より前のすべての8.0リリース

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。

シスコは、この脆弱性がリリース7.2より前のCisco WLCソフトウェアリリースには影響を与えないことを確認しました。また、この脆弱性がCisco WLCソフトウェアリリース8.1以降には影響を与えないことも確認しました。

セキュリティ侵害の痕跡

この脆弱性が不正利用されると、該当するデバイスがリロードされ、クラッシュファイルが生成される可能性があります。Cisco Technical Assistance Center(TAC)に連絡してクラッシュファイルを確認し、この脆弱性の不正利用によってデバイスが侵害されていないかどうかを確認してください。

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リリースしています。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、アクセスまたはその他の方法で使用した場合、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場合は、 http://www.cisco.com/go/psirt の Cisco Security Advisories and Responses アーカイブや後続のアドバイザリを参照して、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 Technical Assistance Center（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/c/ja_jp/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

本項に示すように、適切なリリースにアップグレードする必要があります。本アドバイザリは以下のアドバイザリを含むコレクションの一部です。これらも考慮した上、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。

- cisco-sa-20160420-bdos:CiscoワイヤレスLANコントローラのDoS脆弱性
- cisco-sa-20160420-htrd:CiscoワイヤレスLANコントローラのHTTP解析におけるDoS脆弱性
- cisco-sa-20160420-wlc:CiscoワイヤレスLANコントローラ管理インターフェイスのDoS脆弱性

次の表では、左の列にCisco WLCソフトウェアのメジャーリリースを示します。中央の列が示すのは、本アドバイザリに記載された脆弱性によるメジャー リリースへの影響の有無、また、本脆弱性に対する修正を含む最初のマイナー リリースです。右の列は、メジャー リリースがこのコレクションのアドバイザリに記載した何らかの脆弱性に該当するかどうか、また、これらすべての脆弱性に対する修正を含む最初のリリースを示します。

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。

Cisco WLCソフトウェア メジャー リリース	First Fixed Release for この脆弱性	First Fixed Release for この脆弱性および すべての脆弱性は 勧告集
7.2	8.0.132.0	8.0.132.0
7.3	8.0.132.0	8.0.132.0

7.4	7.4.140.0(MD)	8.0.132.0
7.5	8.0.132.0	8.0.132.0
7.6	8.0.132.0	8.0.132.0
8.0	8.0.115.0(ED)	8.0.132.0

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。

出典

この脆弱性はシスコ内部でのテストによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160420-htrd

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2016年4月20日

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。