Cisco IOS Software Queue Wedge Denial of Service Vulnerability

Advisory ID: cisco-sa-20130925-wedge

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-wedge

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。

Revision 1.0

For Public Release 2013 September 25 16:00 UTC (GMT)

目次

要約

Cisco IOS ソフトウェアの T1/E1 ドライバ キューの実装面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によってインターフェイス ウェッジが発生させられ、接続の切断、ルーティング プロトコルの隣接関係の喪失が引き起こされ、結果的にサービス拒否（DoS）シナリオが発生する可能性があります。

この脆弱性は、T1/E1 ドライバ キューの不適切な実装に起因します。攻撃者は、該当のインターフェイス ドライバを介してバースト トラフィックを送信することで、この脆弱性を不正利用できます。この脆弱性が繰り返し悪用されると、DoS 状態が発生する可能性があります。

この脆弱性を軽減する回避策があります。

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-20130925-wedge
注：2013 年 9 月 25 日の Cisco IOS ソフトウェア セキュリティ アドバイザリ バンドル公開には

、8 件のセキュリティ アドバイザリが含まれています。これらのアドバイザリはすべて、Cisco IOS ソフトウェアの脆弱性に対処するものです。各 Cisco IOS ソフトウェア セキュリティ アドバイザリには、そのアドバイザリで詳述された脆弱性を修正する Cisco IOS ソフトウェア リリース、および 2013 年 9 月にバンドル公開したすべての Cisco IOS ソフトウェアの脆弱性を修正する Cisco IOS ソフトウェア リリースを記載しています。

個別の公開リンクは、次のリンクにある「Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication」に掲載されています。

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep13.html

該当製品

脆弱性が認められる製品

T1/E1 インターフェイス モジュール シグナリングが設定されている該当の Cisco IOS ソフトウェア バージョンが稼働しているシスコ デバイスには、脆弱性が存在します。
デバイスが脆弱になるのは、次の条件をすべて満たしている場合です。

- T1/E1 チャネル グループ用に設定されているインターフェイス コントローラが、該当するハイレベル データ リンク制御 32（HDLC32）ドライバを使用している
- T1/E1 コントローラ クロック ソースが、**回線**または**内部**用に設定されている

注： 該当する HDLC32 ドライバが使用されているのは、Cisco 1900、2900、3900 シリーズ サービス統合型ルータ（ISR）用の VWIC2 インターフェイス カードのみです。

Cisco IOS デバイスで、HDLC32 ドライバを使用しているコントローラに T1/E1 シグナリングが設定されているかどうかを判別するには、 **show controllers** コマンドを実行します。

この脆弱性の影響を受ける Cisco IOS デバイスの例を示します。このデバイスでは、T1 シグナリング用に設定されているインターフェイス Serial0/0/0 に HDLC32 ドライバが使用されているため（「Hardware is HDLC32」の出力に示されています）、脆弱性が存在します。

```
Router#show controllers Serial0/0/0:0
Interface Serial0/0/0:0
Hardware is HDLC32
< >
```

注：VWIC2 インターフェイス カードに使用されている HDLC32 ドライバの脆弱性は、Cisco High-Level Data Link Control ネットワーク プロトコルのカプセル化に固有のものではありません。VWIC2 インターフェイス カードでサポートされているカプセル化タイプは、いずれも脆弱性を引き起こします。

Cisco IOS デバイス上の T1/E1 インターフェイスに設定されているクロック ソース タイプを判別するには、 **show controllers T1/E1** コマンドを発行します。
次の例は、ライン クロック ソースが設定されている Cisco IOS デバイスの E1 インターフェイスを示しています。

```
Router#show controllers e1
E1 0 is up.
Applique type is Channelized E1 - balanced
!---
Framing is CRC4, Line Code is HDB3, Clock Source is Line Primary.
!---
```

シスコ製品で稼働している Cisco IOS ソフトウェア リリースを確認するには、デバイスにログインし **show version** コマンドを実行してシステム バナーを表示させます。「Internetwork Operating System Software」、「Cisco IOS Software」あるいはこれらに類似するシステム バナーによってデバイスで Cisco IOS ソフトウェアが稼働していることを確認できます。その後ろにイメージ名が括弧の間に表示され、続いてバージョンと Cisco IOS ソフトウェア リリース名が表示されます。他のシスコ デバイスでは、**show version** コマンドがない場合や、表示が異なる場合があります。

次の例は、シスコ製品で Cisco IOS ソフトウェア リリース 15.0(1)M1 が稼働し、インストールされているイメージ名が C3900-UNIVERSALK9-M であることを示しています。

```
Router> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 by prod_rel_teamRouter> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 by prod_rel_team
```

Cisco IOS ソフトウェアのリリース命名規則の追加情報は以下のリンクにある「White Paper: Cisco IOS and NX-OS Software Reference Guide」で確認できます。
http://www.cisco.com/web/about/security/intelligence/ios-ref.html

脆弱性が認められない製品

Cisco IOS XR ソフトウェアは、このアドバイザリで説明されている脆弱性の影響を受けません。

Cisco IOS XE ソフトウェアは、このアドバイザリで説明されている脆弱性の影響を受けません。

この脆弱性の影響を受ける他のシスコ製品は、現在確認されていません。

詳細

Cisco IOS ソフトウェアの T1/E1 ドライバ キューの実装面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によってインターフェイス ウェッジが発生させられ、接続の切断、ルーティング プロトコルの隣接関係の喪失が引き起こされ、結果的にサービス拒否（DoS）シナリオが発生する可能性があります。

この脆弱性は、T1/E1 ドライバ キューの不適切な実装に起因します。攻撃者は、該当のインターフェイス ドライバを介してバースト トラフィックを送信することで、この脆弱性を不正利用できます。この脆弱性が繰り返し悪用されると、DoS 状態が発生する可能性があります。

デバイスが脆弱になるのは、HDLC32 ドライバを使用しているインターフェイスに T1/E1 シグナリングが設定されている場合です。

該当するインフラストラクチャの知識を持つ攻撃者は、脆弱なデバイスを経由してネットワーク パケットのバースト プロファイルを送信することで、この脆弱性を不正利用できます。この脆弱性を不正利用すると、攻撃者は出力インターフェイスの送信キューをウェッジすることができます。

この脆弱性を軽減する回避策があります。

脆弱性があると見なされているデバイス上では、有効なネットワーク トラフィックによってこの脆弱性が引き起こされる場合があります。攻撃者は、この脆弱性を不正利用するために設定した、インターフェイスから出力されるネットワーク パケットのバースト プロファイルを送信できます。このインターフェイス キュー ウェッジからの回復には、デバイスのリロードが必要です。

インターフェイス キュー ウェッジとは、Cisco IOS ルータやスイッチが特定のパケットを受信してキューに格納した際に、処理エラーによってキューからパケットを削除できなくなるという脆弱性クラスの 1 つです。

キュー ウェッジと、Cisco IOS ソフトウェア上でブロックされたインターフェイスを特定するのに使用可能ないくつかの検出メカニズムの詳細（SNMP を使用してこの状態を検出する方法に関するホワイト ペーパーを含む）については、次のリンクを参照してください。
http://blogs.cisco.com/security/comments/cisco_ios_queue_wedges_explained/

この脆弱性は、Cisco Bug ID CSCub67465（ 登録ユーザ専用 ）として文書化され、Common Vulnerabilities and Exposures（CVE）ID として CVE-2013-5477 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/

CSCub67465 - Cisco IOS Software Queue Wedge Denial of Service Vulnerability Calculate the environmental score of					
CVSS Base Score - **7.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

この脆弱性が不正利用されると、接続の切断、ルーティング プロトコルの隣接関係の喪失、およびその他の DoS シナリオを引き起こす可能性があるインターフェイス キュー ウェッジが発生します。またこの脆弱性が繰り返し不正利用されることにより、長時間にわたって DoS 状態が続きます。

ソフトウェア バージョンおよび修正

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･ ＜塔eナンス プロバイダーにお問い合わせください。

Cisco IOS ソフトウェア

Cisco IOS ソフトウェア テーブル（下記）の各行は Cisco IOS ソフトウェア トレインを示します。あるトレインが脆弱性を含む場合、修正を含む最初のリリースは「First Fixed Release」列に示されます。「First Fixed Release for All Advisories in the September 2013 Bundled Publication」列は、その Cisco IOS ソフトウェア セキュリティ アドバイザリ バンドル公開で公開済みであるすべての脆弱性を修正する最初のリリースを示します。可能な限り、最新のリリースにアップグレードすることを推奨します。

Cisco IOS ソフトウェア チェッカーを利用して、特定の Cisco IOS ソフトウェア リリースに対応したシスコのセキュリティ アドバイザリを検索することができます。このツールは次の Cisco Security Intelligence Operations（SIO）ポータルで利用できます。

http://tools.cisco.com/security/center/selectIOSVersion.x

Major Release	Availability of Repaired Releases	
Affected 12.0-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the September 2013 Cisco IOS Software Security Advisory Bundled Publication
There are no affected 12.0 based releases		
Affected 12.2-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the September 2013 Cisco IOS Software Security Advisory Bundled Publication
12.2EX	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2EY	Not vulnerable	Vulnerable; First fixed in Release 15.2S
12.2EZ	Not vulnerable	Releases prior to 12.2(60)EZ2 are vulnerable; Releases 12.2(60)EZ2 and later are not vulnerable.First fixed in Release 15.0SE
12.2IRB	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRC	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRD	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRE	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRF	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRG	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IRH	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IRI	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IXG	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IXH	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2MC	Not vulnerable	Vulnerable; First fixed in Release 15.1M
12.2MRA	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2MRB	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SB	Not vulnerable	12.2(33)SB15
12.2SCA	Not vulnerable	Vulnerable; First fixed in Release 12.2SCH
12.2SCB	Not vulnerable	Vulnerable; First fixed in Release 12.2SCH
12.2SCC	Not vulnerable	Vulnerable; First fixed in Release 12.2SCH
12.2SCD	Not vulnerable	Vulnerable; First fixed in Release 12.2SCH
12.2SCE	Not vulnerable	Vulnerable; First fixed in Release 12.2SCH
12.2SCF	Not vulnerable	Vulnerable; First fixed in Release 12.2SCH
12.2SCG	Not vulnerable	Vulnerable; First fixed in Release 12.2SCH
12.2SCH	Not vulnerable	12.2(33)SCH1
12.2SE	Not vulnerable	12.2(55)SE8
12.2SEG	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2SG	Not vulnerable	

		12.2(53)SG10; available December 2013 *
12.2SGA	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SM	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SQ	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SRA	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2SRB	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2SRC	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2SRD	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2SRE	Not vulnerable	12.2(33)SRE9
12.2STE	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SV	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SVD	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SVE	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SW	Not vulnerable	Vulnerable; First fixed in Release 15.1M
12.2SXF	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SXH	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SXI	Not vulnerable	12.2(33)SXI12
12.2SXJ	Not vulnerable	12.2(33)SXJ6
12.2SY	Not vulnerable	Vulnerable; First fixed in Release 15.0SY
12.2WO	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2XNA	Please see Cisco IOS XE Software Availability	Please see Cisco IOS XE Software Availability
12.2XNB	Please see Cisco IOS XE Software Availability	Please see Cisco IOS XE Software Availability
12.2XNC	Please see Cisco IOS XE Software Availability	Please see Cisco IOS XE Software Availability
12.2XND	Please see Cisco IOS XE Software Availability	Please see Cisco IOS XE Software Availability
12.2XNE	Please see Cisco IOS XE Software Availability	Please see Cisco IOS XE Software Availability
12.2XNF	Please see Cisco IOS XE Software Availability	Please see Cisco IOS XE Software Availability
12.2XO	Not vulnerable	Vulnerable; contact your support organization per the

		instructions in Obtaining Fixed Software section of this advisory.
12.2ZYA	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
Affected 12.3-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2013 Cisco IOS Software Security Advisory Bundled Publication**
There are no affected 12.3 based releases		
Affected 12.4-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2013 Cisco IOS Software Security Advisory Bundled Publication**
There are no affected 12.4 based releases		
Affected 15.0-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2013 Cisco IOS Software Security Advisory Bundled Publication**
15.0EA	Not vulnerable	15.0(2)EA1
15.0EB	Not vulnerable	Vulnerable; migrate to any release in 15.2E
15.0EC	Not vulnerable	Vulnerable; migrate to any release in 15.2E
15.0ED	Not vulnerable	Note: Releases prior to 15.0(2)ED1 are vulnerable; Releases 15.0(2)ED1 and later are not vulnerable.
15.0EH	Not vulnerable	Not vulnerable
15.0EJ	Not vulnerable	Not vulnerable
15.0EX	Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.0EY	Not vulnerable	15.0(2)EY2
15.0EZ	Not vulnerable	Only Release 15.0(2)EZ is vulnerable
15.0M	Vulnerable; First fixed in Release 15.1M	Vulnerable; First fixed in Release 15.1M
15.0MR	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.0S	Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	Vulnerable; First fixed in Release 15.1S Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.0SE	Not vulnerable	15.0(2)SE4
15.0SG	Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory. Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.0SQA	Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.0SQB	Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.0SY	Not vulnerable	15.0(1)SY5
15.0XA	Vulnerable; First fixed in Release 15.1M	Vulnerable; First fixed in Release 15.1M
15.0XO	Not vulnerable	Vulnerable; contact your support organization per the

	Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	instructions in Obtaining Fixed Software section of this advisory. Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
Affected 15.1-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2013 Cisco IOS Software Security Advisory Bundled Publication**
15.1EY	Not vulnerable	Vulnerable; First fixed in Release 15.2S
15.1GC	Vulnerable; First fixed in Release 15.1M	Vulnerable; First fixed in Release 15.1M
15.1M	15.1(4)M7	15.1(4)M7
15.1MR	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.1MRA	Not vulnerable	15.1(3)MRA2
15.1S	Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.1(3)S6 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.1SG	Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.1(2)SG1 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.1SNG	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.1SNH	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.1SNI	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.1SVD	Not vulnerable	Not vulnerable
15.1SVE	Not vulnerable	Not vulnerable
15.1SVF	Not vulnerable	Not vulnerable
15.1SY	Not vulnerable	15.1(1)SY2; Available on 28-OCT-13 15.1(2)SY
15.1T	Vulnerable; First fixed in Release 15.1M	Vulnerable; First fixed in Release 15.1M
15.1XO	Not vulnerable	Not vulnerable
Affected 15.2-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2013 Cisco IOS Software Security Advisory Bundled Publication**
15.2E	Not vulnerable	Not vulnerable
15.2GC	15.2(4)GC	Vulnerable; migrate to any release in 15.4T
15.2JA	15.2(4)JA1	15.2(4)JA1
15.2JAX	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.2JB	15.2(2)JB2	15.2(2)JB2
15.2JN	Not vulnerable	Not vulnerable
15.2M	15.2(4)M3	15.2(4)M4
15.2S	Cisco IOS XE devices: Please see	15.2(4)S4

	Cisco IOS XE Software Availability	Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.2SA	Not vulnerable	15.2(2)SA
15.2SNG	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.2SNH	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.2SNI	Not vulnerable	Vulnerable; First fixed in Release 15.3S
15.2T	15.2(2)T4 15.2(3)T4	15.2(3)T4
Affected 15.3-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2013 Cisco IOS Software Security Advisory Bundled Publication**
15.3M	Not vulnerable	Not vulnerable
15.3S	Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.3(2)S2 15.3(3)S Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.3T	15.3(1)T2 15.3(2)T	15.3(1)T2 15.3(2)T1

* Cisco Catalyst 4500 Supervisor Engine 6-E/6L-E 搭載の Cisco Catalyst 4500 シリーズ スイッチは、 Cisco IOS ソフトウェア リリース 15.1SG に移行できます。

Cisco IOS XR ソフトウェア

Cisco IOS XR ソフトウェアは、2013 年 9 月の Cisco IOS Software Security Advisory バンドル公開に含まれている脆弱性の影響を受けません。

Cisco IOS XE ソフトウェア

Cisco IOS XE ソフトウェアは、このアドバイザリで説明されている脆弱性の影響を受けません。

Cisco IOS XE ソフトウェア リリースと Cisco IOS ソフトウェア リリースのマッピングについては、『Cisco IOS XE 2 Release Notes』、『Cisco IOS XE 3S Release Notes』、『Cisco IOS XE 3SG Release Notes』を参照してください。

回避策

ハードウェアのアップグレードを選択できる場合、可能な回避策としては、VWIC2 インターフェイス カードの代わりに VWIC3-T1/E1 または HWIC-T1/E1 インターフェイス カードを使用する方法があります。
あるいは、T1/E1 コントローラが**クロック ソース回線**用に設定されていて、コントローラでチャネル グループが 1 つしか設定されていない場合は、可能な回避策として**クロック ソース回線を単独で**設定する方法があります。

次の方法で、この脆弱性を識別できます。

Cisco IOS Embedded Event Manager（EEM）

脆弱性のある Cisco IOS デバイス上で、ツール コマンド言語（TCL）に基づく組み込みイベント マネージャ（EEM）ポリシーを利用すると、この脆弱性によって引き起こされたインターフェイス キュー ウェッジを識別して、検出することができます。このポリシーによって、管理者は Cisco IOS デバイスのインターフェイスをモニタできるほか、インターフェイス入力キューがいっぱいになると、それを検出できます。Cisco IOS EEM がこの脆弱性による不正利用の可能性を検出すると、それに反応してポリシーがネットワーク管理者にアラートを送信し、それを受けて管理者は、入力キューをクリアするためにデバイスのアップグレード、適切な移行、またはリロードを行うことを判断できます。

TCL スクリプトは、次のリンクの「Cisco Beyond: Embedded Event Manager（EEM）Scripting Community」からダウンロードできます。 https://supportforums.cisco.com/docs/DOC-19337

また、Cisco Security Blog に記載されている「Cisco IOS のキュー ウェッジについて」も参照してください。 http://blogs.cisco.com/security/cisco_ios_queue_wedges_explained/

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。

この脆弱性はサポート ケースの解決中に発見されました。

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-20130925-wedge

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 E 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	2013-September-25	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/en/US/products/products_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。