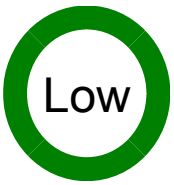
DLSwの脆弱性



アドバイザリーID : cisco-sa-20070110-dlsw CVE-2007-0199
初公開日 : 2007-01-10 16:00
バージョン 1.2 : Final
CVSSスコア : 3.3
回避策 : No Workarounds available
Cisco バグ ID : CSCsf28840

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。

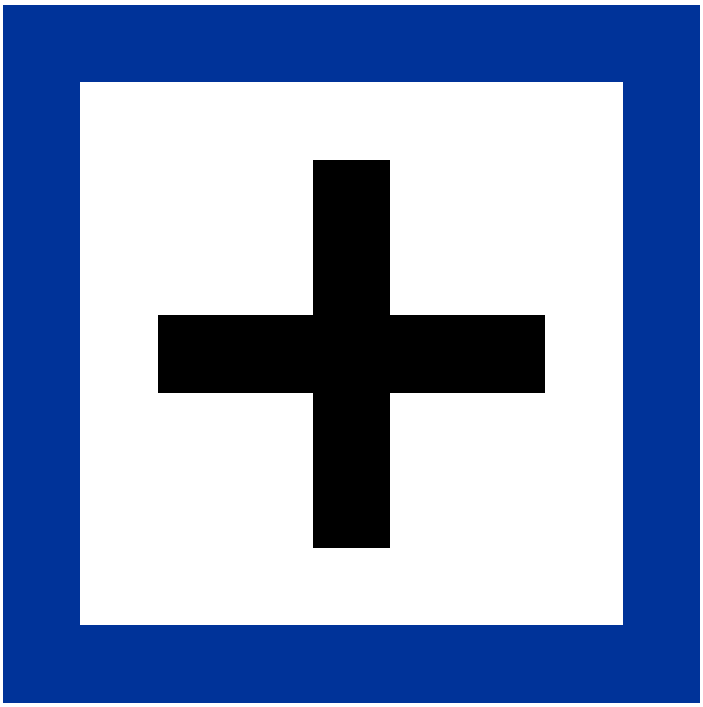
概要

Cisco IOSのデータリンクスイッチング(DLSw)機能には脆弱性が存在し、DLSwメッセージに無効な値があるとDLSwデバイスがリロードされる可能性があります。この脆弱性の不正利用に成功するには、攻撃者がデバイスへのDLSw接続を確立できる必要があります。

この脆弱性には回避策があります。詳細については、次の「回避策」のセクションを参照してください。

このアドバイザリは、
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070110-dlsw で公開されています。

該当製品



脆弱性のある製品

このセキュリティアドバイザリは、DLSw用に設定されたCisco IOSソフトウェアバージョン11.0 ~ 12.4を実行するすべてのシスコ製品に適用されます。DLSw機能が含まれていても有効になっていないシステムは影響を受けません。

DLSw用に設定されたルータには、ローカルDLSwピアを定義する設定に行があります。この定義は、show running-configコマンドを発行し、次のような行を探すことにより確認できます。

```
dlsw local-peer peer-id
```

Cisco IOSデバイスでDLSwが有効になっているかどうかを確認するには、イネーブルモードでshow dlsw statisticsコマンドを発行して、次のような出力を探すこともできます。

```
<#root>

Router#

show dlsw statistics

DLSw+ Control Queue Statistics:
 SNA Control Queue (count/max/dropped):      (0/0/0)
 Netbios Control Queue (count/max/dropped): (0/0/0)
 Other Control Queue (count/max/dropped):    (0/100/0)
 Critical Control Queue (count/max):         (0/0)

DLSw+ Border Peer Caching Statistics:

        0 Border Peer Frames processed
        0 Border frames found Local
        0 Border frames found Remote
        0 Border frames found Group Cache
```

DLSwが設定されていないデバイスは、出力のないコマンドプロンプトに戻るだけです。

DLSw機能をサポートしていないデバイスでは、次のような出力が返されます。

```
<#root>

Router#

show dlsw statistics

               ^
% Invalid input detected at '^' marker.
```

下記の「ソフトウェアバージョンと修正」セクションに記載されるバージョンより前のCisco IOSのバージョンには、脆弱性が存在する可能性があります。

シスコ製品で稼働しているCisco IOSソフトウェアのバージョンを確認するには、デバイスにログインし、show versionコマンドを発行してシステムバナーを表示します。Cisco IOS ソフトウェアは「Internetwork Operating System Software」または単に「IOS」と表示されます。出力の次の行では、イメージ名がカッコで囲まれて表示され、その後に「Version」とIOSリリース名が続きます。その他の Cisco デバイスには show version コマンドがないか、異なる出力が返されます。

次の例は、IOSリリース12.3(6)が稼働し、インストールされているイメージ名がC3640-I-Mであるシスコ製品を示しています。

```
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-I-M), Version 12.3(6), RELEASE SOFTWARE (fc3)
```

次の例は、IOSリリース12.3(11)T3を実行し、イメージ名がC3845-ADVIPSERVICESK9-Mの製品を示しています。

```
Cisco IOS Software, 3800 Software (C3845-ADVIPSERVICESK9-M), Version 12.3(11)T3,
 RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
```

Cisco IOSリリースの命名に関する詳細については、http://www.cisco.com/warp/public/620/1.htmlを参照してください。

他のシスコ製品において、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るものは現在確認されていません。

脆弱性を含んでいないことが確認された製品

脆弱性が存在しないことが確認された製品には、DLSwが設定されていないデバイスが含まれます。

詳細

データリンクスイッチング(DLSw)は、IBM Systems Network Architecture(SNA)およびNetwork Basic Input/Output System(NetBIOS)トラフィックをIPネットワーク上で転送する手段を提供します。

DLSw通信の確立には、いくつかの運用段階が含まれます。

1. フェーズ1では、DLSwピアがTCPポート2065または2067を介して相互に2つのTCP接続を確立します。これらのTCP接続は、DLSw通信の基盤となります。
2. 接続が確立されると、DLSwパートナーはフェーズ2でサポートされる機能のリストを交換します。これにより、ピアが同じオプションを使用することが保証されます。これは、DLSwパートナーが異なるベンダーで製造されている場合に特に重要です。
3. 次に、DLSwパートナーはSNAまたはNetBIOSエンドシステム間に回線を確立し、情報フレームはこの回線を流れることができます。

脆弱性は、DLSw用に設定された特定のCisco IOSソフトウェアリリースに存在します。接続が確立された後、機能交換中にデバイスが無効なオプションを受信すると、リロードが発生する可能性があります。

この脆弱性は、Cisco Bug ID CSCsf28840(登録ユーザ専用)に記載されています。

脆弱性スコア評価の詳細

Cisco では、Common Vulnerability Scoring System（CVSS）に基づき、このアドバイザリで説明されている脆弱性のスコアを評価しました。

Cisco では基本スコアと現状スコアを評価します。お客様はこれらを用いて環境評価スコア（Environmental Score）を算出し、個々のネットワークにおける脆弱性の影響度を導き出すことができます。

Cisco PSIRT は、すべてのケースにおける重みを「標準」に設定します。特定の脆弱性の環境的影響を判断する際には、重みパラメータを適用することを推奨します。

CVSS は、脆弱性の重大度を伝える標準ベースのスコア評価方式であり、対応の緊急度や優先度を判断するのに役立ちます。

シスコは、http://www.cisco.com/web/about/security/intelligence/cvss-qandas.htmlでCVSSに関するFAQを提供しています。

また、シスコはhttps://sec.cloudapps.cisco.com/security/center/cvssCalculator.xで個々のネットワークの環境影響度を計算するCVSS計算ツールを提供しています。

CSCsf28840(登録ユーザ専用)						
CVSS 基本スコア： 3.3						
攻撃元区分	攻撃条件の複雑さ	[Authentication]	機密性への影響	完全性への影響	可用性への影響	影響の重み
Remote	低い	不要	なし	なし	完了	Normal
CVSS 現状スコア - 2.7						

攻撃される可能性	利用可能な対策のレベル	Report Confidence
機能する	正式	確認済

回避策

緩和策または修正の効果は、製品の組み合せ、ネットワーク トポロジ、トラフィックの動作、組織のミッションなど、お客様の状況によって異なります。該当する製品とリリースは多岐に渡るので、サービス プロバイダーやサポート機関に連絡し、ネットワーク内で使用するのに最も適した緩和策や修正を確認してから、実際に配備することを推奨いたします。

ネットワーク内部の Cisco のデバイスに展開できる追加の緩和策については、このアドバイザリに関連する Cisco 適用対応策速報（https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20070110-dlsw）を参照してください。

明示的に定義されたDLSwピアの設定

リモートピアが定義されていない状態でDLSwが設定されている場合は、接続の一端で無差別モードで動作している必要があります。無差別モードでは、任意のデバイスがルータとのDLSwピアの確立を試行できる可能性があります。悪意のある接続を防ぐために、dlsw remote-peerコマンドでDLSwピアを明示的に定義して、無差別モードを不要にすることができます。

修正済みソフトウェア

アップグレードを検討する場合は、[http://www.cisco.com/go/psirt と後続のアドバイザリも参照して、問題の解決状況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。](http://www.cisco.com/go/psirt)

いずれの場合も、アップグレードする機器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しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。情報に不明な点がある場合は、Cisco Technical Assistance Center（TAC）または契約を結んでいるメンテナンス プロバイダーにお問い合せください。

Cisco IOS ソフトウェアの表（下掲）の各行には、リリース トレインとそれに対応するプラットフォームまたは製品が記載されています。特定のリリース トレインに脆弱性がある場合は、修正を含む最初のリリース（「第 1 修正済みリリース」）とそれぞれの提供日が「リビルド」列と「メンテナンス」列に記載されます。特定の列に記されているリリースよりも古い（第 1 修正済みリリースより古い）トレインに含まれるリリースが稼働しているデバイスは脆弱であることが確認されています。このようなリリースは、少なくとも、示されているリリース以上（最初の修正リリース ラベル以上）にアップグレードしてする必要があります。

「リビルド」および「メンテナンス」という用語の詳細については、次のURLを参照してください。http://www.cisco.com/warp/public/620/1.html。

メジャー リリース	修正済みリリースの入手可能性	
該当する 12.0 ベースのリリース	リビルド	メンテナンス
12.0	脆弱性あり、12.2(46)に移行。2007年5月10日に入手可能	
12.0S		12.0(18)S
12.0SZ	脆弱性あり、12.0(23)S以降に移行	
12.0T	脆弱性あり、12.2(46)に移行。2007年5月10日に入手可能	
12.0WC	12.0(5)WC17	
12.0XA	脆弱性あり、12.2(46)に移行。2007年5月10日に入手可能	
12.0XC	脆弱性あり、12.2(46)に移行。2007年5月10日に入手可能	
12.0XD	脆弱性あり、12.2(46)に移行。2007年5月10日に入手可能	
12.0XE	脆弱性あり、12.1(26)E8に移行	

12.0XG	脆弱性あり、12.2(46)に移行。2007年5月10日に入手可能	
12.0XH	脆弱性あり、12.2(46)に移行。2007年5月10日に入手可能	
12.0XI	脆弱性あり、12.2(46)に移行。2007年5月10日に入手可能	
12.0XJ	12.0(4)XJ5	
12.0XK	脆弱性あり、12.2(46)に移行。2007年5月10日に入手可能	
12.0XN	脆弱性あり、12.2(46)に移行。2007年5月10日に入手可能	
12.0XQ	脆弱性あり、12.2(46)に移行。2007年5月10日に入手可能	
12.0XR	脆弱性あり、12.2(46)に移行。2007年5月10日に入手可能	
12.0XT	脆弱性あり。TACに連絡	
該当する 12.1 ベースのリリース	リビルド	メンテナンス
12.1	脆弱性あり、12.2(46)に移行。2007年5月10日に入手可能	
12.1AA	脆弱性あり、12.2(46)に移行。2007年	

	5月10日に入手可能	
12.1E	12.1(26)E8	
	12.1(27b)E2（2007年6月25日に入手可能）	
12.1EC	脆弱性あり、12.2(4)BC1以降に移行	
12.1EX	脆弱性あり、12.1(26)E8に移行	
12.1EZ	脆弱性あり、12.1(26)E8に移行	
12.1T	脆弱性あり、12.2(46)に移行。2007年5月10日に入手可能	
12.1XA	脆弱性あり、12.2(46)に移行。2007年5月10日に入手可能	
12.1XC	脆弱性あり、12.2(46)に移行。2007年5月10日に入手可能	
12.1XD	脆弱性あり、12.2(46)に移行。2007年5月10日に入手可能	
12.1XE	12.1(1)XE1	
12.1XG	脆弱性あり、12.3(21)以降に移行	
12.1XH	脆弱性あり、12.2(46)に移行。2007年5月10日に入手可能	

12.1XI	脆弱性あり、12.2(46)に移行。2007年5月10日に入手可能	
12.1XJ	脆弱性あり、12.3(21)以降に移行	
12.1XM	脆弱性あり、12.3(21)以降に移行	
12.1XP	脆弱性あり、12.3(21)以降に移行	
12.1XQ	脆弱性あり、12.3(21)以降に移行	
12.1XS	脆弱性あり、12.2(46)に移行。2007年5月10日に入手可能	
12.1XT	12.1(3)XT2	
12.1XV	12.1(5)XV1	
12.1XW	脆弱性あり、12.2(46)に移行。2007年5月10日に入手可能	
12.1XX	脆弱性あり、12.2(46)に移行。2007年5月10日に入手可能	
12.1XY	脆弱性あり、12.2(46)に移行。2007年5月10日に入手可能	
12.1XZ	脆弱性あり、12.2(46)に移行。2007年5月10日に入手可能	
12.1YA	脆弱性あり、12.3(21)以降に移行	

12.1YB	脆弱性あり、12.3(21)以降に移行	
12.1YD	脆弱性あり、12.3(21)以降に移行	
12.1YI	脆弱性あり、12.3(21)以降に移行	
該当する 12.2 ベースのリリース	リビルド	メンテナンス
12.2		12.2(46)（2007年5月10日に入手可能）
12.2B	脆弱性あり、12.4(12)以降に移行	
12.2BW	脆弱性あり、12.3(21)以降に移行	
12.2BY	脆弱性あり、12.4(12)以降に移行	
12.2DD	脆弱性あり、12.4(12)以降に移行	
12.2DX	脆弱性あり、12.4(12)以降に移行	
12.2IXA	脆弱性あり、12.2(18)IXC以降に移行	
12.2IXB	脆弱性あり、12.2(18)IXC以降に移行	
12.2MC	脆弱性あり、12.4(12)以降に移行	
12.2S		12.2(30)S

12.2SB	12.2(28)SB6	
	12.2(31)SB2	
12.2SBC	脆弱性あり、12.2(31)SB2以降に移行	
12.2SRA	12.2(33)SRA2	
12.2SU	脆弱性あり、12.4(12)以降に移行	
12.2SV		12.2(26)SV
12.2SW	12.2(25)SW9	
12.2SX	脆弱性あり、12.2(18)SXE6bに移行	
12.2SXA	脆弱性あり、12.2(18)SXE6bに移行	
12.2SXB	脆弱性あり、12.2(18)SXE6bに移行	
12.2SXD	脆弱性あり、12.2(18)SXE6bに移行	
12.2SXE	12.2(18)SXE6b	
12.2SXF	12.2(18)SXF8	
12.2SY	脆弱性あり、12.2(18)SXE6bに移行	
12.2SZ	脆弱性あり、12.2(30)S以降に移行	

12.2T	脆弱性あり、12.3(21)以降に移行	
12.2TPC	脆弱性あり。TACに連絡	
12.2XA	脆弱性あり、12.3(21)以降に移行	
12.2XB	12.2(2)XB17	
12.2XC	脆弱性あり、12.4(12)以降に移行	
12.2XD	脆弱性あり、12.3(21)以降に移行	
12.2XG	脆弱性あり、12.3(21)以降に移行	
12.2XH	脆弱性あり、12.3(21)以降に移行	
12.2XJ	脆弱性あり、12.3(21)以降に移行	
12.2XK	脆弱性あり、12.3(21)以降に移行	
12.2XL	脆弱性あり、12.3(21)以降に移行	
12.2XM	脆弱性あり、12.3(21)以降に移行	
12.2XN	脆弱性あり、12.3(21)以降に移行	
12.2XQ	脆弱性あり、12.3(21)以降に移行	
12.2XT	脆弱性あり、12.3(21)以降に移行	

12.2XU	脆弱性あり、12.3(21)以降に移行	
12.2XV	脆弱性あり、12.3(21)以降に移行	
12.2XW	脆弱性あり、12.3(21)以降に移行	
12.2YA	12.2(4)YA10	
12.2YB	脆弱性あり、12.3(21)以降に移行	
12.2YC	脆弱性あり、12.3(21)以降に移行	
12.2YD	脆弱性あり、12.4(12)以降に移行	
12.2YE	脆弱性あり、12.2(30)S以降に移行	
12.2YF	脆弱性あり、12.3(21)以降に移行	
12.2YH	脆弱性あり、12.3(21)以降に移行	
12.2YJ	12.2(8)YJ1	
12.2YL	脆弱性あり、12.4(12)以降に移行	
12.2YM	脆弱性あり、12.4(12)以降に移行	
12.2YN	脆弱性あり、12.4(12)以降に移行	
12.2YT	脆弱性あり、12.3(21)以降に移行	

12.2YU	脆弱性あり、12.4(12)以降に移行	
12.2YV	12.2(11)YV1	
12.2YW	脆弱性あり、12.4(12)以降に移行	
12.2YX	脆弱性あり、12.4(12)以降に移行	
12.2YY	脆弱性あり、12.4(12)以降に移行	
12.2YZ	脆弱性あり、12.2(30)S以降に移行	
12.2ZA	脆弱性あり、12.2(18)SXE6bに移行	
12.2ZB	脆弱性あり、12.4(12)以降に移行	
12.2ZD	脆弱性あり。TACに連絡	
12.2ZE	脆弱性あり、12.3(21)以降に移行	
12.2ZF	脆弱性あり、12.4(12)以降に移行	
12.2ZH	12.2(13)ZH6	
12.2ZJ	脆弱性あり、12.4(12)以降に移行	
12.2ZL	脆弱性あり。TACに連絡	
12.2ZN	脆弱性あり、12.4(12)以降に移行	

12.2ZP	12.2(20)S7以降に移行	
12.2ZU	脆弱性あり。TACに連絡	
12.2ZV	12.2(28a)ZV1	
12.2ZW	脆弱性あり、12.2(33)SRBに移行	
12.2ZX		12.2(28)ZX
該当する 12.3 ベースのリリース	リビルド	メンテナンス
12.3		12.3(21)
12.3B	脆弱性あり、12.4(12)以降に移行	
12.3BW	脆弱性あり、12.4(12)以降に移行	
12.3T	脆弱性あり、12.4(12)以降に移行	
12.3XA	12.3(2)XA5	
12.3XB	脆弱性あり、12.4(12)以降に移行	
12.3XC	12.3(2)XC3	
12.3XD	脆弱性あり、12.4(12)以降に移行	
12.3XE	12.3(2)XE2	

12.3XF	脆弱性あり、12.4(12)以降に移行	
12.3XG	脆弱性あり。TACに連絡	
12.3XH	脆弱性あり、12.4(12)以降に移行	
12.3XI	12.3(7)XI8a	
12.3XJ	脆弱性あり、12.4(11)T1に移行	
12.3XK	脆弱性あり、12.4(12)以降に移行	
12.3XQ	脆弱性あり、12.4(12)以降に移行	
12.3XR	脆弱性あり。TACに連絡	
12.3XU	脆弱性あり、12.4(4)T7以降に移行	
12.3XW	脆弱性あり、12.4(11)T1に移行	
12.3XX	12.3(8)XX2	
12.3YF	脆弱性あり、12.4(11)T1に移行	
12.3YG	12.3(8)YG5	
12.3YH	脆弱性あり、12.4(4)T7以降に移行	
12.3YI	脆弱性あり、12.4(4)T7以降に移行	

12.3YJ	脆弱性あり、12.4(6)T6以降に移行	
12.3YK	脆弱性あり、12.4(4)T7以降に移行	
12.3YM	脆弱性あり。TACに連絡	
12.3YQ	脆弱性あり、12.4(6)T6以降に移行	
12.3YT	脆弱性あり、12.4(4)T7以降に移行	
12.3YU	脆弱性あり。TACに連絡	
12.3YX	脆弱性あり、12.4(11)T1に移行	
12.3YZ	脆弱性あり。TACに連絡	
該当する 12.4 ベースのリリース	リビルド	メンテナンス
12.4	12.4(7d)	
	12.4(8c)	
	12.4(10a)	12.4(12)
12.4T	12.4(4)T7	
	12.4(6)T6	
	12.4(9)T3	

	12.4(11)T1	
12.4XA	脆弱性あり、12.4(6)T6以降に移行	
12.4XB	脆弱性あり。TACに連絡	
12.4XC	12.4(4)XC6	
12.4XD	12.4(4)XD5	
12.4XE	脆弱性あり。TACに連絡	

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

この脆弱性は、MWR InfoSecurityのMartyn Ruks氏によってシスコに報告され、最初は2006年8月にDEFCONで提示されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070110-dlsw

改訂履歴

リビジョン 1.2	2007年 4月20日	リリース情報と日付を修正しました。特に12.2(46)の修正に関して修正しました。
リビジョン 1.1	2007年 1月12日	12.4(11)T1の修正済みリリース日

リビジョン 1.0	2007年 1月10日	初版リリース

利用規約

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も示唆するものではありません。 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、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

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。