DLSw 脆弱性

Low

アドバイザリーID : cisco-sa-20070110-dlsw

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

CVE-2007-0199

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

DLSw メッセージの無効 な値が DLSw デバイスのリロードという結果に終る可能性がある Cisco IOS の Data-Link Switching （ DLSw; データリンク スイッチング ） 機能で存在 する脆弱性。 この脆弱性の不正利用の成功は攻撃者がデバイスへの DLSw 接続を確立できることを必要とします。

回避策 下記の例で説明されているようにこの脆弱性のために、利用可能 な 回避策があります。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070110-dlsw で掲示されます

該当製品

脆弱性のある製品

この Security Advisory は Cisco IOS ソフトウェア バージョン 11.0 〜 DLSw のために設定される 12.4 を実行するすべてのシスコ製品に適用します。 システムに DLSw 機能がある、有効になるそれが影響を受けていませんありませんが。

DLSw のために設定されるルータはローカル DLSw ピアを定義するコンフィギュレーションの行を備えています。 この定義はコマンド **show running-config** を発行することおよび次と同じような行を探すことによって参照される場合があります:

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

に類似した イネーブル モードおよび探された出力で間 DLSw が Cisco IOSデバイスで有効になったかどうか確認するために、**show dlsw statistics コマンドを**発行することもまた可能性のあるです:

```
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 のために設定されないデバイスは出力無しでコマンド プロンプトに単に戻ります。

DLSw 機能をサポートしないデバイスはに類似した出力を戻します:

```
Router#show dlsw statistics
              ^
% Invalid input detected at '^' marker.
```

ソフトウェア バージョン および 修正 下記の例にリストされるバージョン前の Cisco IOS のどのバージョンでも脆弱かもしれません。

デバイスに Cisco製品、ログインで動作する Cisco IOSソフトウェアのバージョンを判別し、システムバナーを表示する **show version コマンドを**発行するため。 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。 出力次の行で、イメージ名は「バージョンに」先行しているかっこと IOSリリース名の間で表示する。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 C3640-I-M のインストール済みイメージ名前と IOS リリース 12.3(6) を実行する Cisco製品を指定したものです:

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

次の例は C3845-ADVIPSERVICESK9-M のイメージ名と IOS リリース 12.3(11)T3 を実行する製品を示します:

```
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 リリース指名についてのその他の情報は http://www.cisco.com/warp/public/620/1.html で見つけることができます。

その他のCisco製品は現在このアドバイザリで当たる脆弱性から影響を受けるために知られていません。

脆弱性を含んでいないことが確認された製品

脆弱ではないために確認される製品は DLSw のために設定されないデバイスが含まれています。

詳細

Data-Link Switching（DLSw; データリンク スイッチング）は IPネットワーク上の IBM システム ネットワーク アーキテクチャ（SNA）および Network Basic Input/Output System（NetBIOS（NetBIOS over IP））トラフィックの転送の方法を提供します。

DLSw 通信を確立することは複数の操作上ステージを含みます。

1. フェーズ1、DLSw 同位 確立する TCP ポート 2065 または 2067 による 2 つの TCP 接続互いに。 それらの TCP 接続は DLSw 通信に基礎を提供します。
2. 接続が確立された後、DLSw パートナーはフェーズ 2 のサポートされた機能のリストを交換します。 これはように同位 使用同じオプションするのを助けます。 これは DLSw パートナーが異なるベンダーによって製造されるとき特に重要です。
3. 次に、DLSw パートナーは SNA または NetBIOS（NetBIOS over IP）エンド システム間の回線を接続し、インフォメーションフレームは回線にフローできます。

DLSw のために設定された場合ある特定の Cisco IOS ソフトウェア リリースで存在 する脆弱性。接続は確立された後、機能の間の無効 な オプションが交換するデバイス レシーブがもしリロードが発生することは可能性のあるです。

この脆弱性は Cisco バグ ID CSCsf28840（登録ユーザのみ）で文書化されています。

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。

Cisco は http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html で CVSS に関する追加質問に答えるために FAQ を提供しました。

Cisco はまた http://tools.cisco.com/security/center/cvssCalculator.x で個々のネットワークのための環境影響の計算を助けるように CVSS カルキュレータを提供しました。

CSCsf28840（登録ユーザのみ）						
CVSS 基本スコア：3.3						
攻撃元区分	攻撃条件の複雑さ	認証	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	不要	なし	なし	Complete	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。

Cisco 機器に適用可能な追加の軽減策については以下の "Cisco Applied Intelligence companion document" より入手可能です。
http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20070110-dlsw

設定 明示的に定義された DLSw 同位

DLSw が定義されるリモートピア無しで設定される場合接続の一端の混合モードでオペレーティングである必要があります。 混合モードはどのデバイスでもルータとの DLSw ピアを確立するように試みることができるように可能にする可能性があります。 悪意のある接続を防ぐために、DLSw 同位は混合モードの必要性を取除く **dlsw remote-peer コマンド**で明示的に定義されるかもしれません。

修正済みソフトウェア

ソフトウェアのアップグレードを検討する際には、http://www.cisco.com/go/psirt およびそれ以降のアドバイザリも参照して、起こりうる障害と完全なアップグレード ソリューションを判断してください

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	Vulnerable; 12.2(46) への移行する; 利用可能 な 10-May-07	
12.0S		12.0(18)S
12.0SZ	Vulnerable; 12.0(23)S またはそれ以降への移行する	
12.0T	Vulnerable; 12.2(46) への移行する; 利用可能 な 10-May-07	
12.0WC	12.0(5)WC17	
12.0XA	Vulnerable; 12.2(46) への移行する; 利用可能 な 10-May-07	
12.0XC	Vulnerable; 12.2(46) への移行する; 利用可能 な 10-May-07	
12.0XD	Vulnerable; 12.2(46) への移行する; 利用可能 な 10-May-07	
12.0XE	Vulnerable; 12.1(26)E8 への移行する	
12.0XG	Vulnerable; 12.2(46) への移行する; 利用可能 な 10-May-07	
12.0XH	Vulnerable; 12.2(46) への移行する; 利用可能 な 10-May-07	

12.0XI	Vulnerable; 12.2(46) への移行する; 利用可能 な 10-May-07	
12.0XJ	12.0(4)XJ5	
12.0XK	Vulnerable; 12.2(46) への移行する; 利用可能 な 10-May-07	
12.0XN	Vulnerable; 12.2(46) への移行する; 利用可能 な 10-May-07	
12.0XQ	Vulnerable; 12.2(46) への移行する; 利用可能 な 10-May-07	
12.0XR	Vulnerable; 12.2(46) への移行する; 利用可能 な 10-May-07	
12.0XT	Vulnerable; contact TAC	
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	Vulnerable; 12.2(46) への移行する; 利用可能 な 10-May-07	
12.1AA	Vulnerable; 12.2(46) への移行する; 利用可能 な 10-May-07	
12.1E	12.1(26)E8	
	12.1(27b)E2; 利用可能 な 25-Jun-07	
12.1EC	Vulnerable; 12.2(4)BC1 またはそれ以降への移行する	
12.1EX	Vulnerable; 12.1(26)E8 への移行する	
12.1EZ	Vulnerable; 12.1(26)E8 への移行する	
12.1T	Vulnerable; 12.2(46) への移行する; 利用可能 な 10-May-07	
12.1XA	Vulnerable; 12.2(46) への移行する; 利用可能 な 10-May-07	
12.1XC	Vulnerable; 12.2(46) への移行する; 利用可能 な 10-May-07	
12.1XD	Vulnerable; 12.2(46) への移行する; 利用可能 な 10-May-07	
12.1XE	12.1(1)XE1	
12.1XG	Vulnerable; 12.3(21) またはそれ以降への移行する	
12.1XH	Vulnerable; 12.2(46) への移行する; 利用可能 な 10-May-07	
12.1XI	Vulnerable; 12.2(46) への移行する; 利用可能 な 10-May-07	
12.1XJ	Vulnerable; 12.3(21) またはそれ以降への移行する	
12.1XM	Vulnerable; 12.3(21) またはそれ以降への移行する	

12.1XP	Vulnerable; 12.3(21) またはそれ以降への移行する	
12.1XQ	Vulnerable; 12.3(21) またはそれ以降への移行する	
12.1XS	Vulnerable; 12.2(46) への移行する; 利用可能 な 10-May-07	
12.1XT	12.1(3)XT2	
12.1XV	12.1(5)XV1	
12.1XW	Vulnerable; 12.2(46) への移行する; 利用可能 な 10-May-07	
12.1XX	Vulnerable; 12.2(46) への移行する; 利用可能 な 10-May-07	
12.1XY	Vulnerable; 12.2(46) への移行する; 利用可能 な 10-May-07	
12.1XZ	Vulnerable; 12.2(46) への移行する; 利用可能 な 10-May-07	
12.1YA	Vulnerable; 12.3(21) またはそれ以降への移行する	
12.1YB	Vulnerable; 12.3(21) またはそれ以降への移行する	
12.1YD	Vulnerable; 12.3(21) またはそれ以降への移行する	
12.1YI	Vulnerable; 12.3(21) またはそれ以降への移行する	
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); 利用可能 な 10-May-07
12.2B	Vulnerable; 12.4(12) またはそれ以降への移行する	
12.2BW	Vulnerable; 12.3(21) またはそれ以降への移行する	
12.2BY	Vulnerable; 12.4(12) またはそれ以降への移行する	
12.2DD	Vulnerable; 12.4(12) またはそれ以降への移行する	
12.2DX	Vulnerable; 12.4(12) またはそれ以降への移行する	
12.2IXA	Vulnerable; 12.2(18)IXC またはそれ以降への移行する	
12.2IXB	Vulnerable; 12.2(18)IXC またはそれ以降への移行する	
12.2MC	Vulnerable; 12.4(12) またはそれ以降への移行する	
12.2S		12.2(30)S
12.2SB	12.2(28)SB6	
	12.2(31)SB2	

12.2SBC	Vulnerable; 12.2(31)SB2 またはそれ以降への移行する	
12.2SRA	12.2(33)SRA2	
12.2SU	Vulnerable; 12.4(12) またはそれ以降への移行する	
12.2SV		12.2(26)SV
12.2SW	12.2(25)SW9	
12.2SX	Vulnerable; 12.2(18)SXE6b への移行する	
12.2SXA	Vulnerable; 12.2(18)SXE6b への移行する	
12.2SXB	Vulnerable; 12.2(18)SXE6b への移行する	
12.2SXD	Vulnerable; 12.2(18)SXE6b への移行する	
12.2SXE	12.2(18)SXE6b	
12.2SXF	12.2(18)SXF8	
12.2SY	Vulnerable; 12.2(18)SXE6b への移行する	
12.2SZ	Vulnerable; 12.2(30)S またはそれ以降への移行する	
12.2T	Vulnerable; 12.3(21) またはそれ以降への移行する	
12.2TPC	Vulnerable; contact TAC	
12.2XA	Vulnerable; 12.3(21) またはそれ以降への移行する	
12.2XB	12.2(2)XB17	
12.2XC	Vulnerable; 12.4(12) またはそれ以降への移行する	
12.2XD	Vulnerable; 12.3(21) またはそれ以降への移行する	
12.2XG	Vulnerable; 12.3(21) またはそれ以降への移行する	
12.2XH	Vulnerable; 12.3(21) またはそれ以降への移行する	
12.2XJ	Vulnerable; 12.3(21) またはそれ以降への移行する	
12.2XK	Vulnerable; 12.3(21) またはそれ以降への移行する	
12.2XL	Vulnerable; 12.3(21) またはそれ以降への移行する	
12.2XM	Vulnerable; 12.3(21) またはそれ以降への移行する	
12.2XN	Vulnerable; 12.3(21) またはそれ以降への移行する	

12.2XQ	Vulnerable; 12.3(21) またはそれ以降への移行する
12.2XT	Vulnerable; 12.3(21) またはそれ以降への移行する
12.2XU	Vulnerable; 12.3(21) またはそれ以降への移行する
12.2XV	Vulnerable; 12.3(21) またはそれ以降への移行する
12.2XW	Vulnerable; 12.3(21) またはそれ以降への移行する
12.2YA	12.2(4)YA10
12.2YB	Vulnerable; 12.3(21) またはそれ以降への移行する
12.2YC	Vulnerable; 12.3(21) またはそれ以降への移行する
12.2YD	Vulnerable; 12.4(12) またはそれ以降への移行する
12.2YE	Vulnerable; 12.2(30)S またはそれ以降への移行する
12.2YF	Vulnerable; 12.3(21) またはそれ以降への移行する
12.2YH	Vulnerable; 12.3(21) またはそれ以降への移行する
12.2YJ	12.2(8)YJ1
12.2YL	Vulnerable; 12.4(12) またはそれ以降への移行する
12.2YM	Vulnerable; 12.4(12) またはそれ以降への移行する
12.2YN	Vulnerable; 12.4(12) またはそれ以降への移行する
12.2YT	Vulnerable; 12.3(21) またはそれ以降への移行する
12.2YU	Vulnerable; 12.4(12) またはそれ以降への移行する
12.2YV	12.2(11)YV1
12.2YW	Vulnerable; 12.4(12) またはそれ以降への移行する
12.2YX	Vulnerable; 12.4(12) またはそれ以降への移行する
12.2YY	Vulnerable; 12.4(12) またはそれ以降への移行する
12.2YZ	Vulnerable; 12.2(30)S またはそれ以降への移行する
12.2ZA	Vulnerable; 12.2(18)SXE6b への移行する
12.2ZB	Vulnerable; 12.4(12) またはそれ

	以降への移行する	
12.2ZD	Vulnerable; contact TAC	
12.2ZE	Vulnerable; 12.3(21) またはそれ以降への移行する	
12.2ZF	Vulnerable; 12.4(12) またはそれ以降への移行する	
12.2ZH	12.2(13)ZH6	
12.2ZJ	Vulnerable; 12.4(12) またはそれ以降への移行する	
12.2ZL	Vulnerable; contact TAC	
12.2ZN	Vulnerable; 12.4(12) またはそれ以降への移行する	
12.2ZP	12.2(20)S7 またはそれ以降への移行する	
12.2ZU	Vulnerable; contact TAC	
12.2ZV	12.2(28a)ZV1	
12.2ZW	Vulnerable; 12.2(33)SRB への移行する	
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	Vulnerable; 12.4(12) またはそれ以降への移行する	
12.3BW	Vulnerable; 12.4(12) またはそれ以降への移行する	
12.3T	Vulnerable; 12.4(12) またはそれ以降への移行する	
12.3XA	12.3(2)XA5	
12.3XB	Vulnerable; 12.4(12) またはそれ以降への移行する	
12.3XC	12.3(2)XC3	
12.3XD	Vulnerable; 12.4(12) またはそれ以降への移行する	
12.3XE	12.3(2)XE2	
12.3XF	Vulnerable; 12.4(12) またはそれ以降への移行する	
12.3XG	Vulnerable; contact TAC	
12.3XH	Vulnerable; 12.4(12) またはそれ以降への移行する	
12.3XI	12.3(7)XI8a	
12.3XJ	Vulnerable; 12.4(11)T1 への移行する	
12.3XK	Vulnerable; 12.4(12) またはそれ以降への移行する	
12.3XQ	Vulnerable; 12.4(12) またはそれ	

	以降への移行する	
12.3XR	Vulnerable; contact TAC	
12.3XU	Vulnerable; 12.4(4)T7 またはそれ以降への移行する	
12.3XW	Vulnerable; 12.4(11)T1 への移行する	
12.3XX	12.3(8)XX2	
12.3YF	Vulnerable; 12.4(11)T1 への移行する	
12.3YG	12.3(8)YG5	
12.3YH	Vulnerable; 12.4(4)T7 またはそれ以降への移行する	
12.3YI	Vulnerable; 12.4(4)T7 またはそれ以降への移行する	
12.3YJ	Vulnerable; 12.4(6)T6 またはそれ以降への移行する	
12.3YK	Vulnerable; 12.4(4)T7 またはそれ以降への移行する	
12.3YM	Vulnerable; contact TAC	
12.3YQ	Vulnerable; 12.4(6)T6 またはそれ以降への移行する	
12.3YT	Vulnerable; 12.4(4)T7 またはそれ以降への移行する	
12.3YU	Vulnerable; contact TAC	
12.3YX	Vulnerable; 12.4(11)T1 への移行する	
12.3YZ	Vulnerable; contact TAC	
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	Vulnerable; 12.4(6)T6 またはそれ以降への移行する	
12.4XB	Vulnerable; contact TAC	
12.4XC	12.4(4)XC6	
12.4XD	12.4(4)XD5	
12.4XE	Vulnerable; contact TAC	

不正利用事例と公式発表

この脆弱性は MWR InfoSecurity のマーティン Ruks によって Cisco に報告され、尊厳な 2006 年に DEFCON で最初に示されました。

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070110-dlsw

改訂履歴

リビジョン 1.2	2007-April-20	12.2(46) 修正の訂正されたリリース 情報および日付、特に。
リビジョン 1.1	2007-January-12	12.4(11)T1 の訂正されたリリース日付
リビジョン 1.0	2007-January-10	初版リリース

利用規約