Cisco IOSの不正なOSPFパケットによるリロード

アドバイザリーID : cisco-sa-20040818-ospf CVE-2004-1454
初公開日 : 2004-08-18 15:00
バージョン 1.4 : Final
回避策 : No Workarounds available
Cisco バグ ID : CSCec16481

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

Open Shortest Path First(OSPF)プロトコルに対してイネーブルになっているInternetwork Operating System(IOS)®ードを実行しているシスコデバイスは、不正なOSPFパケットによるサービス拒否(DoS)攻撃に対して脆弱です。OSPFプロトコルはデフォルトでは有効になっていません。

この脆弱性は、12.0S、12.2、および12.3に基づくCisco IOSリリーストレインにのみ存在します。12.0、12.1メインラインに基づくリリース、および12.0より前のすべてのCisco IOSイメージは影響を受けません。

シスコはこの脆弱性に対処する無償ソフトウェアを提供しています。

影響を緩和するための回避策があります。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040818-ospfで確認できます。

該当製品

このセクションには、該当製品に関する詳細が掲載されています。

脆弱性のある製品

この脆弱性は、12.0S、12.2、および12.3ベースのリリーストレインに対するコード変更によって引き起こされ、これらのトレインには脆弱性が存在します。脆弱性のあるリリーストレインを実行し、OSPFプロセスを実行するすべてのシスコデバイスに脆弱性が存在します。

脆弱性が存在しない一部のリリーストレインについては、以下で明示的に説明します。下記に

記載されていないリリーストレインには脆弱性はありません。

リリーストレイン	脆弱性のあるバージョン
10.xベースのリリース	脆弱性なし
11.xベースのリリース	脆弱性なし
12.0ベースのリリース（12.0.Sベースのリリースを除く）	脆弱性なし
12.1ベースのリリース	脆弱性なし
12.0.S	12.0(22)S以降
12.0.SX	12.0(23)SX以降
12.0.SY	12.0(22)SY以降
12.0.SZ	12.0(23)SZ以降
12.2 メインライン	脆弱性なし
12.2.B	12.2(15)B以降
12.2.BC	12.2(15)BC以降
12.2.BX	12.2(15)BX以降
12.2.BZ	12.2(15)BZ以降

12.2.CX	12.2(15)CX以降
12.2.EW	12.2(18)EW以降
12.2.MC	12.2(15)MC1以降
12.2.S	12.2(18)S以降
12.2.SE	12.2(18)SE以降
12.2.SV	12.2(18)SV以降
12.2.SW	12.2(18)SW以降
12.2.SZ	12.2(14)SZ以降
12.2.T	12.2(15)T以降
12.2.YU	12.2(11)YU以降
12.2.YV	12.2(11)YV以降
12.2.ZD	12.2(13)ZD以降
12.2.ZE	12.2(13)ZE以降
12.2.ZF	12.2(13)ZF以降
12.2.ZG	12.2(13)ZG以降

12.2.ZH	12.2(13)ZH 以降
12.2.ZJ	12.2(15)ZJ以降
12.2.ZK	12.2(15)ZK以降
12.2.ZL	12.2(15)ZL以降
12.2.ZN	12.2(15)ZN以降
12.2.ZO	12.2(15)ZO以降
12.3	すべての12.3リリース
12.3.B	すべての12.3.Bリリース
12.3.BW	すべての12.3.BWリリース
12.3.T	すべての12.3.Tリリース
12.3.XA	すべての12.3.XAリリース
12.3.XB	すべての12.3.XBリリース
12.3.XC	すべての12.3.XCリリース

12.3.XE	すべての12.3.XEリリース

OSPFプロセスを実行しているCiscoデバイスの設定には、プロセス番号を定義する行があります。これは、show running-configコマンドを発行すると表示できます。

<#root>

```
router ospf {process number}
```

Cisco 製品で稼働しているソフトウェアを確認するには、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。 出力の次の行には、カッコに囲まれたイメージ名が表示され、その後にバージョンと Cisco 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、シスコ製品でCisco IOSリリース12.0(3)が稼働し、インストールされているイメージ名がC2500-IS-Lであることを示しています。

```
Cisco Internetwork Operating System Software IOS (TM)
2500 Software (C2500-IS-L), Version 12.0(3), RELEASE SOFTWARE
```

リリーストレインラベルは「12.0」です。 次の例は、Cisco IOSリリース12.0(2a)T1が稼働し、イメージ名がC2600-JS-MZである製品を示しています。

```
Cisco Internetwork Operating System Software IOS (tm)
C2600 Software (C2600-JS-MZ), Version 12.0(2a)T1, RELEASE SOFTWARE (fc1)
```

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

脆弱性を含んでいないことが確認された製品

次の製品には脆弱性が存在しないことが確認されています。

- Cisco IOSを実行していない製品は該当しません。

- Cisco IOSバージョン12.0以前（12.0 Sを除く）、12.1メインライン、および12.2メインラインを実行している製品には脆弱性はありません。
- 上記の表に記載されていないIOSリリーストレインを実行している製品には、脆弱性は存在しません。
- OSPFが設定されていないCisco IOSのバージョンを実行している製品には、脆弱性は存在しません。

詳細

OSPFは、RFC 2328で定義されているルーティングプロトコルです。自律システム(AS)内のIPルーティングを管理するように設計されています。OSPFパケットはIPプロトコル番号89を使用します。

脆弱性はOSPFパケットの処理に存在し、不正利用されるとシステムのリロードを引き起こす可能性があります。

OSPFはマルチキャストパケットだけでなくユニキャストパケットも処理する必要があるため、この脆弱性はリモートから悪用される可能性があります。攻撃者は、一度にローカルセグメント上の複数のシステムをターゲットにすることもできます。

この脆弱性の影響を緩和するには、「回避策」セクションで説明されているOSPF認証を使用できます。OSPF認証の使用は、セキュリティのベストプラクティスとして強く推奨されています

不正なOSPFパケットを受信したシスコデバイスはリセットされ、完全に機能するまでに数分かかることがあります。この脆弱性が繰り返し悪用されると、長時間にわたるDOS攻撃が発生する可能性があります。この問題は、Bug ID CSCec16481に記載されています。

回避策

回避策の効果は、製品の組み合わせ、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回避策を確認してから、実際に配備することを推奨いたします。

この脆弱性の影響を軽減するには、複数の回避策があります。

OSPF認証の使用

回避策としてOSPF認証を使用できます。有効なキーのないOSPFパケットは処理されません。プレーンテキスト認証には固有の弱点があるため、MD5認証を強く推奨します。プレーンテキスト認証では、認証キーは暗号化されずにネットワーク経由で送信されるため、ローカルネットワークセグメントの攻撃者がパケットをスニッフィングしてキーをキャプチャする可能性があります。

OSPF認証についての詳細は、http://www.cisco.com/en/US/tech/tk365/technologies_configuration_example09186a0080094069.shtmlを参照してください。

インフラストラクチャ アクセス コントロール リスト

ネットワークを移動するトラフィックをブロックするのは往々にして困難ですが、インフラストラクチャ デバイスに送られてはならないトラフィックを識別し、ネットワークの境界でそのトラフィックをブロックすることは可能です。インフラストラクチャ ACL はネットワーク セキュリティのベスト プラクティスと考えられており、ここでの特定の脆弱性の回避策としてだけでなく、優れたネットワーク セキュリティへの長期的な付加機能として考慮する必要があります。ホワイトペーパー『Protecting Your Core: Infrastructure Protection Access Control Lists』には、インフラストラクチャ保護ACLのガイドラインと推奨される導入方法が記載されています。http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml。

修正済みソフトウェア

表の各行に、リリース群、および対象のプラットフォームまたは製品を示します。特定のリリーストレインに脆弱性が存在する場合は、修正を含む最初のリリースとそれぞれの提供予定日が「Rebuild」、「Interim」、および「Maintenance」の各列に表示されます。場合によっては、特定のリリースのリビルドが計画されていない場合があります。この場合、「Not scheduled」というラベルが付きます。 特定の列のリリースより前（最初の修正リリースより前）のトレインのリリースを実行しているデバイスは脆弱であることが確認されており、少なくとも示されたリリースまたは以降のバージョン（最初の修正リリースのラベルより後）にアップグレードする必要があります。

リリースを選択するときは、次の定義を念頭においてください。

- メンテナンス：テストを重ね、推奨される、表の特定の行にあるラベルのリリースです。
- リビルド：同じトレインの以前のメンテナンスリリースまたはメジャーリリースから構築され、特定の脆弱性に対する修正が含まれています。テストの回数は少なくなりますが、修復に必要な最小限の変更のみが含まれています。シスコでは、この脆弱性に対処するためにメインライントレインのリビルドを数種類提供していますが、最新のメンテナンスリリースのみをメインライントレインで実行することを強く推奨します。
- 暫定：メンテナンスリリース間の定期的な間隔で構築され、テストの頻度は少なくなります。暫定イメージは、脆弱性に対処する適切なリリースが他にない場合にのみ選択し、可能な限り早急に次のメンテナンスリリースにアップグレードする必要があります。暫定リリースは製品としては提供されず、通常は、Cisco Technical Assistance Center（TAC）によって事前に手配されない限り、CCO からダウンロードできません。

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。情報が不明な場合は、次の表に示すように、Cisco TACに連絡して支援を求めてください。

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	Interim	メンテナンス
12.0(22)S以降	12.0(22)S6		
	12.0(23)S5		
	12.0(24)S2c		
	12.0(24)S4		
	12.0(25)S1d		
	12.0(25)S2		
	12.0(26)S1		12.0(27)S
12.0(23)SX以降	12.0(25)SX2		
12.0(22)SY以降	12.0(23)S5以降に移行		
12.0(23)SZ以降			12.0(27)SZ
該当する 12.2 ベースのリリース	リビルド	Interim	メンテナンス

12.2(15)B以降	12.3(4)T以降に移行		
12.2(15)BC以降	12.2(15)BC1c		
	12.2(15)BC2		
12.2(15)BX以降	12.3(7)XI1以降に移行		
12.2(15)BZ以降	12.3(7)XI1以降に移行		
12.2(15)CX以降	12.2(15)BC2以降に移行		
12.2(18)EW	12.2(18)EW1		12.2(20)EW
12.2(15)MC1以降	12.2(15)MC2aリクエストに応じて利用可能		
12.2(18)S以降	12.2(20)S 12.2(18)S5		
12.2(18)SE以降			12.2(20)SE
12.2(18)SV以降			12.2(22)SV
12.2(18)SW以降			12.2(20)SW

12.2(14)SZ以降	12.2(20)S4以降に移行		
12.2(15)T以降	12.2(15)T8		
12.2(11)YU以降	12.3(4)T以降に移行		
12.2(11)YV以降	12.3(4)T以降に移行		
12.2(13)ZD以降	12.3T以降に移行		
12.2(13)ZE以降	12.3以降に移行		
12.2(13)ZF以降	12.3(4)T以降に移行		
12.2(13)ZG以降	12.3(4)T以降に移行		
12.2(13)ZH 以降	12.3(4)T以降に移行		
12.2(15)ZJ以降	12.3T以降に移行		
12.2(15)ZK以降	12.2(15)ZK2		
12.2(15)ZL以降	12.3(7)T以降に移行		
12.2(15)ZN以降	12.3(2)T4以降に		

	移行		
12.2(15)ZO以降	12.2(15)T8以降に移行		
該当する 12.3 ベースのリリース	リビルド	Interim	メンテナンス
12.3	12.3(3f)		12.3(5)
12.3B	12.3(5a)B		
12.3BW	12.3B以降に移行		
12.3T	12.3(2)T4		12.3(4)T
12.3XA	12.3(7)T以降に移行		
12.3XB	12.3(2)XB3		
12.3XC	12.3(8)T以降に移行		
12.3XE	12.3(8)T以降に移行		

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco 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やその公表は確認しておりません。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040818-ospf

改訂履歴

リビジョン 1.4	2005年 3月29日	「12.2(15)BX以降」の「該当する12.2ベースリリース」の「ソフトウェアバージョンおよび修正」セクションで、リビルドセル「12.2(16)BX Migrate to 12.3(7)XI1 or later」を「Migrate to 12.3(7)XI1 or later」に変更しました。
リビジョン 1.3	2004年 8月27日	「攻撃者がこの脆弱性を悪用するには、いくつかのパラメータを知っている必要があります。これらは、対象のインターフェイスに設定されているOSPFエリア番号、ネットマスク、hello、および deadタイマーです。
リビジョン 1.2	2004年 8月21日	IOS修正済みソフトウェアテーブルの「12.2(18)S以降」の行で、12.2(20)SをMaintenanceカラムからRebuildカラムに移動しました。
リビジョン 1.1	2004年 8月20日	「ソフトウェアバージョンと修正」セクションの表の上にテキストを追加。 IOS修正済みソフトウェアテーブルの「12.2(18)EW」行で、「Maintenance」列に12.2(20)EWが追加されました。IOS修正済みソフトウェアの表で、表の見出しから「*」と「**」が削除されました。

リビジョン 1.0	2004年 8月18日	初回公開リリース

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。