Cisco IOS 不正 な OSPFパケット原因リロード

severity

アドバイザリーID : cisco-sa-20040818-ospf

初公開日 : 2004-08-18 15:00

バージョン 1.4 : Final

回避策 : Yes

Cisco バグ ID : CSCec16481

CVE-2004-1454

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

インターネットワークオペレーティングシステム（IOS）Â® を実行する Ciscoデバイスは Open Shortest Path First（OSPF）プロトコルのために有効に されて 不正 な OSPFパケットからのサービス拒絶（DoS）攻撃に脆弱であり。 OSPFプロトコルはデフォルトで有効に なりません。

脆弱性は 12.0S、12.2、および 12.3 に基づいて Cisco IOSの一連のリリースにだけあります。 12.0、12.1 メインラインおよび 12.0 前にすべての Cisco IOSイメージに基づくリリースは影響を受けていません。

Cisco はこの脆弱性に対処するためにフリーソフトを使用できるようにしました。

利用可能 な 回避策が効果を軽減するためにあります。

このアドバイザリは 818-ospf で利用できます。

該当製品

修正済みソフトウェア

この脆弱性は 12.0S に託されたコード変更、12.2、および脆弱にこれらのトレインをする 12.3 基づいたリリース トレインによってもたらされました。 脆弱なリリース トレインを実行し、OSPFプロセスを実行するすべての Ciscoデバイスは脆弱です。

脆弱ではないいくつかのリリース トレインは説明のために明示的に下記に記載されています。 下記に述べられないリリース トレインは脆弱ではないです。

リリース トレイン	脆弱なバージョン
10.x はリリースを基づかせていま	脆弱性なし

した	
11.x はリリースを基づかせていました	脆弱性なし
12.0 基づいたリリース (12.0.S によって基づくリリースを除く)	脆弱性なし
12.1 基づいたリリース	脆弱性なし
12.0.S	12.0(22)S およびそれ以降
12.0.SX	12.0(23)SX およびそれ以降
12.0.SY	12.0(22)SY およびそれ以降
12.0.SZ	12.0(23)SZ およびそれ以降
12.2 メインライン	脆弱性なし
12.2.B	12.2(15)B およびそれ以降
12.2.BC	12.2(15)BC およびそれ以降
12.2.BX	12.2(15)BX およびそれ以降
12.2.BZ	12.2(15)BZ およびそれ以降
12.2.CX	12.2(15)CX およびそれ以降
12.2.EW	12.2(18)EW およびそれ以降
12.2.MC	12.2(15)MC1 およびそれ以降
12.2.S	12.2(18)S およびそれ以降
12.2.SE	12.2(18)SE およびそれ以降
12.2.SV	12.2(18)SV およびそれ以降
12.2.SW	12.2(18)SW およびそれ以降
12.2.SZ	12.2(14)SZ およびそれ以降
12.2.T	12.2(15)T およびそれ以降
12.2.YU	12.2(11)YU およびそれ以降
12.2.YV	12.2(11)YV およびそれ以降
12.2.ZD	12.2(13)ZD およびそれ以降

12.2.ZE	12.2(13)ZE およびそれ以降
12.2.ZF	12.2(13)ZF およびそれ以降
12.2.ZG	12.2(13)ZG およびそれ以降
12.2.ZH	12.2(13)ZH 以降
12.2.ZJ	12.2(15)ZJ およびそれ以降
12.2.ZK	12.2(15)ZK およびそれ以降
12.2.ZL	12.2(15)ZL およびそれ以降
12.2.ZN	12.2(15)ZN およびそれ以降
12.2.ZO	12.2(15)ZO およびそれ以降
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デバイスは**コマンド show running-config の**発行によって見られる場合があるプロセス数を定義する設定の行を備えています:

```
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 C2500-IS-L のインストール済みイメージ名前と Cisco IOS Release 12.0(3)を実行す

る Cisco製品を指定したものです:

router ospf {process number}

リリース トレイン ラベルは次 の 例が C2600-JS-MZ のイメージ名と Cisco IOS Release 12.0(2a)T1 を実行する製品を示す "12.0." です:

router ospf {process number}

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。

脆弱性を含んでいないことが確認された製品

これらの製品は確認された脆弱です:

- Cisco IOS を実行していない製品は影響を受けていません。
- Cisco IOSバージョン 12.0 およびそれ以前を実行する製品は（ 12.0 S を除いて）、12.1 メインラインおよび 12.2 メインライン 脆弱ではないです。
- 上の表で述べられない IOSの一連のリリースを実行する製品は脆弱ではないです。
- Cisco IOS のバージョンを実行する設定される OSPF がない製品は脆弱ではないです。

改訂履歴

リビジョン 1.4	2005-March-29	ソフトウェア バージョン および 修正 セクションではの下の 12.3(7)XI1 またはそれ以降に移行するために「該当しました 12.3(7)XI1 またはそれ以降に改造セル "12.2(16)BX 移行する」変更された "12.2(15)BX およびそれ以降のための 12.2 ベースのリリース」に「」。
リビジョン 1.3	2004-August-27	文を「攻撃者によって正常にこの脆弱性を不正利用すると知られている複数のパラメータ必要取除きました。 これらはターゲット インターフェイスで」。設定される OSPF エリア番号、ネットマスク、HELLO およびデッド タイマーです 詳細 セクションから。
リビジョン 1.2	2004-August-21	IOS 修正済みソフトウェア 表では、列 "12.2(18)S およびそれ以降のために」、Maintenance カラムから Rebuild カラムに 12.2(20)S を移動しました。
リビジョン 1.1	2004-August-20	ソフトウェア バージョン および 修正 セクションの表の上の追加されたテキスト。 IOS 修正済みソフトウェア 表、なぜなら列 "12.2(18)EW," で Maintenance カラムに 12.2(20)EW を追加しました。 「取除かれた IOS 修正済みソフトウェア 表では*」および

		「**」表見出しから取除きました。
リビジョン 1.0	2004-August-18	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。