不正侵入の毒する DNS キャッシュに脆弱 な複数のシスコ製品

Medium	**アドバイザリーID :** cisco-sa-20080708-dns **初公開日 :** 2008-07-08 18:00 **バージョン 2.1 :** Final **CVSSスコア :** 6.4 **回避策 :** No Workarounds available **Cisco バグ ID :** CSCso81854	CVE-2008-5133 CVE-2008-1447

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

複数のシスコ製品はに DNS キャッシュの毒できる炉 DNS 返事攻撃者をより簡単に可能にするかもしれない、発声する DNS クエリの不十分にランダム化された DNS トランザクション ID および UDP 送信元ポートの使用による不正侵入の毒する DNS キャッシュに脆弱です。

この脆弱性を不正利用するために攻撃者は脆弱 な DNSサーバを回帰的な DNS クエリを行うために引き起こせます必要があります。 従って、ただ保証された いる再帰が許可されない DNSサーバ、またはサーバは、影響を受けていません。

シスコはこれらの脆弱性に対処するソフトウェア アップデートを提供しています。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080708-dns で掲示されます。

この Security Advisory は他の影響を受けた組織からの発表と同時に公開されています。

該当製品

再帰を用いる DNS 応答およびプロセス DNS メッセージをキャッシュする製品は（RD）フラグが設定を DNS プロトコルの実装によって攻撃の毒する DNS キャッシュに脆弱かもしれません望みました。 RD フラグが設定が付いている DNS メッセージを処理する製品はクライアントに代わって尋ねられた質問に答えるように試みます。 製品は DNS プロトコルの脆弱 な 実装を、DNSサーバ 機能が製品のために使用して有効に なる、製品のための DNS 機能は回帰的な DNS クエリ メッセージを処理するために設定されます場合その時だけ影響を受けて。

脆弱性のある製品

以下のシスコ製品は DNSサーバとして機能することができ、DNS の成功するためにいくつかの型に中毒不正侵入をもっと多分キャッシュさせる DNS 実装脆弱性があるためにありました:

- **Cisco IOS ソフトウェア**

  Cisco IOSソフトウェアを実行しているデバイスは脆弱なバージョンを実行すれば、そして DNSサーバとして機能すれば影響を受けています。

  DNSサーバ 機能をサポートする改善される DNS 実装がないし、すべての Cisco IOS ソフトウェア リリースは影響を受けています。 特定の修正済み バージョンについての情報に関しては、ソフトウェア バージョン および 修正 セクションを参照して下さい。

  Cisco IOSソフトウェアを実行しているデバイスはコマンド **IP DNSサーバが**設定にある場合 DNSサーバとして機能するために設定されます。 このコマンドはデフォルトで有効になりません。

- **Cisco Network Registrar**

  すべての Cisco Network Registrarバージョンは影響を受けて、DNS サービスはデフォルトで有効に なります。

  CNR の DNSサーバは Command Line Interface （ CLI ）コマンド **サーバ dns イネーブル開始する再度ブートする**か **dns イネーブル開始する再度ブートする**またはサーバ ページの Web管理インターフェイスによって適切な「開始する」、「停止」、か「リロード」ボタンの選択によって有効に なります。

- **Cisco Application and Content Networking System (ACNS) ソフトウェア**

  すべては Cisco Application and Content Networking System （ ACNS ）ソフトウェア （ ACNS ）バージョン影響を受けています; DNS サービスはデフォルトでディセーブルにされます。

  ACNS はコマンド **dns イネーブルが**設定にある場合 DNSサーバとして機能するために設定されます。

- **Cisco Network Registrar と組み合わせて使用される Cisco グローバルサイトセレクタ**

  より完全な DNS ソリューションを提供することを Cisco Network Registrar ソフトウェアと組み合わせて使用するとき Cisco グローバルサイトセレクタ （ GSS ）は影響を受けています。 修正済みソフトウェアは GSS ソフトウェアのアップデートよりもむしろ Cisco

Network Registrar ソフトウェアのアップデートの形になります。

脆弱性を含んでいないことが確認された製品

DNSサーバ機能を提供しない製品はこの脆弱性から影響を受けません。

Cisco GSS はこの脆弱性からそれ自体影響を受けません。 ただし、それは Cisco Network Registrar ソフトウェアと使用されるとき影響を受けています。

他のシスコ製品においてこのアドバイザリの影響を受けるものは、現在確認されていません。

詳細

インターネットのような TCP/IP に基づいているネットワークの統合部分はドメイン ネーム システム（DNS）です。 、ドメイン ネーム システム（DNS）ホスト名および IP アドレスのマッピングが含まれている階層的 な データベースは単に示されます。 DNS プロトコルは TCP/IPプロトコル スイートの一部で、DNS クライアントが IP アドレスにホスト名を解決するために DNS データベースを問い合わせることを可能にします。

DNS プロトコルを設定する DNS クライアントが送信するクエリに応答する機能があり、DNSサーバはアプリケーションです。（クエリが DNSサーバが保証された いる DNS データベースの部分のためなら DNS クライアントからのクエリを処理するとき、DNSサーバがグローバル な DNS データベースの部分）、またはそれ調べることができる（そうすることを設定すれば、そしてクエリが DNSサーバが保証された いない DNS データベースの部分のためなら他の DNSサーバにクエリを中継で送ることができます。）

DNS クエリの処理と関連付けられる処理時間および帯域幅が理由で、ローカルでほとんどの DNSサーバは他の DNSサーバから届く応答を保存します。 これらの応答がローカルで保存されるエリアは呼ばれます「キャッシュと」。 応答がキャッシュで保存されれば、応答のローカル（キャッシュされた）コピーをリフレッシュするために DNSサーバはある特定の時間の間前に DNSサーバを再度問い合わせなければならないローカルで保存された応答を（「存続可能時間」呼出される使用）できます。

攻撃の毒する DNS キャッシュは DNSサーバの DNS キャッシュのエントリが変更される従ってキャッシュのホスト名と関連付けられる IP アドレスは正しいインポートを指しません攻撃です。 たとえば、www.example.com が IP アドレス 192.168.0.1 にマッピング され、このマッピングが DNSサーバのキャッシュにあれば、このサーバの DNS キャッシュの毒に成功する攻撃者は 10.0.0.1 に www.example.com を代りにマッピング できますかもしれません。 これが起こる場合、www.example.com を参照することを試みているユーザは間違った Webサーバの連絡を終了するかもしれません。

不正侵入の毒する DNS キャッシュが新しくないが、セキュリティ研究者は最近攻撃者が低い複雑な状況ツールおよび低いトラフィック必要条件の不正侵入の毒する正常な DNS キャッシュをマウントすることを可能にする手法を示しました。 この手法は DNS プロトコルのほとんどの実

装の脆弱性につけこみます。 基本的な実装脆弱性は DNS 応答を検証するのに使用される攻撃者が期待値を一致する DNS クエリへの造られた応答を作成することを可能にする DNS トランザクション ID および送信元ポート番号が十分にランダム化されないし、容易に予測することができることです。 DNSサーバはそのような応答が有効であると考慮します。

DNSサーバ 機能を提供する以下のシスコ製品は不正侵入の毒する DNS キャッシュに敏感であるために確認されています:

- Cisco IOS ソフトウェア： Cisco バグ ID CSCso81854 （登録ユーザのみ）で文書化されています脆弱性。
- Cisco Network Registrar: Cisco バグ ID CSCsq01298 （登録ユーザのみ）で文書化されています脆弱性。
- Cisco Application and Content Networking System（ACNS）ソフトウェア（ACNS）: Cisco バグ ID CSCsq21930 （登録ユーザのみ）で文書化されています脆弱性。

この脆弱性よくある脆弱性および公開（CVE） ID CVE-2008-1447 は割り当てられました。

ポート アドレス変換考慮事項

ポート アドレス変換 （PAT）はプライベート ネットワークのマルチプルホストが単一を使用してパブリックネットワークにアクセスするようにするネットワーク アドレス変換（NAT）の形式パブリックIPアドレスです。 これはレイヤ4 情報の、とりわけ TCP および UDP 送信元ポート番号およびチェックサム書き換えによってプライベート ネットワークからのパケットが PAT を行っているネットワークデバイスを横断するので、達成されます。 PAT はネットワーク管理者によって設定され、公共 IP アドレスが限られている状況のファイアウォールおよびルータのようなネットワークデバイスによって実行された。

最初のマルチベンダ DNS アドバイザリは 2008 年 7 月 8 日公開された後そのようなクエリが PAT デバイスを横断するとき DNS クエリを送信 するとき場合によってはランダムソース ポートを使用する DNS 実装への修正が否定できることに検出されました。 この理由は PAT に必要のレイヤ4 書き直しオペレーションを行うときこのような場合ネットワークデバイス実行 PAT が予想できる送信元ポート 割り当て ポリシーを、インクレメンタル アロケーションのような使用することです。 このシナリオの下で、DNS ベンダーがなす修正はプライベート ネットワークを去るとき内部ネットワークで見られる DNS クエリにランダムソース ポート番号があるが、同じクエリにデバイスを通って中継そのトラフィック の 種類によって可能性としては予想できる送信元ポート番号があるので非常に減少することができます。

複数のシスコ製品はこの問題から影響を受け、DNSサーバが PAT モードで動作するこれらの該当製品の 1 つの後ろでそして展開されれば送信元ポート無作為化更新が DNSサーバに加えられても DNS インフラストラクチャはまだ危険な状態にあるかもしれません。

影響を受けたシスコ製品および問題をトラッキングするために作成されたそれぞれ Ciscoバグは次です:

Product	Cisco Bug ID
Cisco PIX（6.3.x およびそれ以前）	CSCsr28354（登録ユーザのみ）
Cisco ASA および Cisco PIX（7.0.x およびそれ以降）	CSCsr28008（登録ユーザのみ）
Firewall Services Module（FWSM; ファイアウォール サービス モジュール）	CSCsr29124（登録ユーザのみ）
Cisco IOS	CSCsr29691（登録ユーザのみ）
Cisco コンテンツ スイッチング モジュール（CSM）	CSCsr61220（登録ユーザのみ）
Ciscoアプリケーション コントロール エンジン（ACE）モジュール	CSCsr98689（登録ユーザのみ）
Ciscoアプリケーション コントロール エンジン（ACE）アプライアンス	CSCsu10546（登録ユーザのみ）

これらのバグのための修正済みソフトウェア 情報はこの文書に追加されません。 その代り、顧客は cisco.com の Bug Toolkit アプリケーションの規則的なサポート チャネルか修正済みソフトウェア 情報を得るのに不具合 トラッキング機能を使用する必要があります。

ACE モジュールおよび ACE アプライアンスを除いて、上記の製品は PAT のために必要である送信元ポート書き直しオペレーションを行うときインクレメンタル送信元ポート 割り当て ポリシーを使用します。 Cisco IOS の場合には、オリジナルソースポートは最初に試されます、そのポートが既に割り当てられて既存の PAT 変換のために使用中それから新しいポートはインクレメンタルに割り当てられ。

ACE モジュールおよび ACE アプライアンスはインクレメンタル送信元ポート アロケーションを使用しません。 ただし、それらは PAT オペレーションの間に予想できる『Source』 を選択 された ポート番号を作るかもしれないハッシュ アルゴリズムを使用します。

その従来の NAT に注意して下さい、すなわち、PAT とは違って、NAT がレイヤ3 情報だけを書き換え、NAT デバイスを横断するパケットのレイヤ4 ヘッダー情報を修正しないので各プライベート IP アドレスのための 1 パブリックIPアドレスを割り当てることはこの問題から、影響を受けません。

回避策

回避策がありません。

DNS に対する不正侵入の識別および軽減についてのその他の情報は Cisco によって加えられる知性 白書「DNS 最良 の 方法に、ネットワーク保護および攻撃 識別」、http://www.cisco.com/web/about/security/intelligence/dns-bcp.html で利用可能あります。

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

Cisco IOSソフトウェア 表 (下記) の各行は Cisco IOS ソフトウェア リリース トレインを指名します。 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 (および、それぞれの予想提供日) が表の「第 1 修正済みリリース」列に記載されます。 「推奨リリース」列には、このアドバイザリが作成された時点で発表されているすべての脆弱性の修正を含むリリースが記載されます。 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。 表の「推奨リリース」列に記載されているリリース、またはそれよりも新しいリリースにアップグレードすることを推奨します。

メジャー リリース	修理されたリリースの Â Â Â Â Â 可用性	
Affected 12.0-Based Releases	**First Fixed Release (修正された最初のリリース)**	**推奨リリース**
12.0	脆弱性なし	Â
12.0DA	脆弱性なし	Â
12.0DB	Release prior to 12.0(7)DB are vulnerable， releases 12.0(7)DB and later are not vulnerable; first fixed in 12.4	12.4(19a) 12.4(19b)
12.0DC	Release prior to 12.0(7)DC are vulnerable， releases 12.0(7)DC and later are not vulnerable; first fixed in 12.4	12.4(19a) 12.4(19b)
12.0S	脆弱性なし	Â
12.0SC	脆弱性なし	Â

12.0SL	脆弱性なし	Â
12.0SP	脆弱性なし	Â
12.0ST	脆弱性なし	Â
12.0SX	脆弱性なし	Â
12.0SY	脆弱性なし	Â
12.0SZ	脆弱性なし	Â
12.0T	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.0W	脆弱性なし	Â
12.0WC	脆弱性あり; contact TAC	Â
12.0WT	脆弱性なし	Â
12.0XA	脆弱性なし	Â
12.0XB	脆弱性なし	Â
12.0XC	脆弱性なし	Â
12.0XD	脆弱性なし	Â
12.0XE	注： Release prior to 12.0(7)XE1 are vulnerable， releases 12.0(7)XE1 and later are not vulnerable;	Â
12.0XF	脆弱性なし	Â
12.0XG	脆弱性なし	Â
12.0XH	脆弱性なし	Â
12.0XI	脆弱性なし	Â
12.0XJ	脆弱性なし	Â
12.0XK	Release prior to 12.0(7)XK2 are vulnerable， releases 12.0(7)XK2 and later are not vulnerable; first fixed in 12.4	12.4(19a) 12.4(19b)
12.0XL	脆弱性なし	Â
12.0XM	脆弱性なし	Â
12.0XN	脆弱性なし	Â
12.0XQ	脆弱性なし	Â
12.0XR	Release prior to 12.0(7)XR1 are vulnerable， releases 12.0(7)XR1 and later are not vulnerable; first fixed in 12.4	12.4(19a) 12.4(19b)
12.0XS	脆弱性なし	Â
12.0XV	脆弱性なし	Â
12.0XW	脆弱性なし	Â
Affected 12.1-Based Releases	**First Fixed Release (修正された最初のリリース)**	**推奨リリース**
12.1	脆弱性あり; first fixed in 12.4	12.4(19a)

		12.4(19b)
12.1AA	脆弱性なし	Â
12.1AX	脆弱性なし	Â
12.1AY	Release prior to 12.1(22)AY1 are vulnerable， releases 12.1(22)AY1 and later are not vulnerable;	12.1(22)EA11
12.1AZ	脆弱性なし	Â
12.1CX	脆弱性なし	Â
12.1DA	脆弱性なし	Â
12.1DB	Release prior to 12.1(4)DB1 are vulnerable， releases 12.1(4)DB1 and later are not vulnerable; first fixed in 12.4	12.4(19a) 12.4(19b)
12.1DC	Release prior to 12.1(4)DC2 are vulnerable， releases 12.1(4)DC2 and later are not vulnerable; first fixed in 12.4	12.4(19a) 12.4(19b)
12.1E	脆弱性なし	Â
12.1EA	Release prior to 12.1(11)EA1 are vulnerable， releases 12.1(11)EA1 and later are not vulnerable;	12.1(22)EA11
12.1EB	脆弱性なし	Â
12.1EC	脆弱性なし	Â
12.1EO	脆弱性なし	Â
12.1EU	脆弱性なし	Â
12.1EV	脆弱性なし	Â
12.1EW	脆弱性なし	Â
12.1EX	注： Release prior to 12.1(8a)EX are vulnerable， releases 12.1(8a)EX and later are not vulnerable;	Â
12.1EY	脆弱性なし	Â
12.1EZ	脆弱性なし	Â
12.1GA	脆弱性なし	Â
12.1GB	脆弱性なし	Â
12.1T	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.1XA	脆弱性なし	Â
12.1XB	脆弱性なし	Â
12.1XC	Release prior to 12.1(1)XC1 are vulnerable， releases 12.1(1)XC1 and later are not vulnerable; first fixed in 12.4	12.4(19a) 12.4(19b)
12.1XD	脆弱性なし	Â

12.1XE	脆弱性なし	Â
12.1XF	脆弱性なし	Â
12.1XG	脆弱性なし	Â
12.1XH	脆弱性なし	Â
12.1XI	脆弱性なし	Â
12.1XJ	脆弱性なし	Â
12.1XK	脆弱性なし	Â
12.1XL	脆弱性なし	Â
12.1XM	脆弱性なし	Â
12.1XN	脆弱性なし	Â
12.1XO	脆弱性なし	Â
12.1XP	脆弱性なし	Â
12.1XQ	脆弱性なし	Â
12.1XR	脆弱性なし	Â
12.1XS	脆弱性なし	Â
12.1XT	脆弱性なし	Â
12.1XU	脆弱性なし	Â
12.1XV	脆弱性なし	Â
12.1XW	脆弱性なし	Â
12.1XX	脆弱性なし	Â
12.1XY	脆弱性なし	Â
12.1XZ	脆弱性なし	Â
12.1YA	脆弱性なし	Â
12.1YB	脆弱性なし	Â
12.1YC	脆弱性なし	Â
12.1YD	脆弱性なし	Â
12.1YE	注： Release prior to 12.1(5)YE1 are vulnerable， releases 12.1(5)YE1 and later are not vulnerable;	12.4(19a) 12.4(19b)
12.1YF	脆弱性なし	Â
12.1YG	脆弱性なし	Â
12.1YH	脆弱性なし	Â
12.1YI	脆弱性なし	Â
12.1YJ	脆弱性なし	Â
Affected 12.2-Based Releases	**First Fixed Release (修正された最初のリリース)**	**推奨リリース**
12.2	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.2B	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)

12.2BC	脆弱性なし	Â
12.2BW	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.2BY	Release prior to 12.2(8)BY are vulnerable， releases 12.2(8)BY and later are not vulnerable; first fixed in 12.4	12.4(19a) 12.4(19b)
12.2BZ	脆弱性なし	Â
12.2CX	脆弱性なし	Â
12.2CY	脆弱性なし	Â
12.2CZ	脆弱性あり; contact TAC	Â
12.2DA	脆弱性なし	Â
12.2DD	脆弱性なし	Â
12.2DX	脆弱性なし	Â
12.2EU	脆弱性なし	Â
12.2EW	脆弱性なし	Â
12.2EWA	脆弱性なし	Â
12.2EX	脆弱性なし	Â
12.2EY	脆弱性なし	Â
12.2EZ	脆弱性なし	Â
12.2FX	脆弱性なし	Â
12.2FY	脆弱性なし	Â
12.2FZ	脆弱性なし	Â
12.2IXA	脆弱性なし	Â
12.2IXB	脆弱性なし	Â
12.2IXC	脆弱性なし	Â
12.2IXD	脆弱性なし	Â
12.2IXE	脆弱性なし	Â
12.2IXF	脆弱性なし	Â
12.2JA	脆弱性なし	Â
12.2JK	脆弱性なし	Â
12.2MB	脆弱性なし	Â
12.2MC	脆弱性なし	Â
12.2S	脆弱性なし	Â
12.2SB	脆弱性なし	Â
12.2SBC	脆弱性なし	Â
12.2SCA	脆弱性なし	Â
12.2SE	脆弱性なし	Â
12.2SEA	脆弱性なし	Â
12.2SEB	脆弱性なし	Â
12.2SEC	脆弱性なし	Â
12.2SED	脆弱性なし	Â

12.2SEE	脆弱性なし	Â
12.2SEF	脆弱性なし	Â
12.2SEG	脆弱性なし	Â
12.2SG	脆弱性なし	Â
12.2SGA	脆弱性なし	Â
12.2SL	脆弱性なし	Â
12.2SM	脆弱性なし	Â
12.2SO	脆弱性なし	Â
12.2SRA	脆弱性なし	Â
12.2SRB	脆弱性なし	Â
12.2SRC	脆弱性なし	Â
12.2SU	脆弱性なし	Â
12.2SV	脆弱性なし	Â
12.2SVA	脆弱性なし	Â
12.2SVC	脆弱性なし	Â
12.2SVD	脆弱性なし	Â
12.2SW	脆弱性なし	Â
12.2SX	脆弱性なし	Â
12.2SXA	脆弱性なし	Â
12.2SXB	脆弱性なし	Â
12.2SXD	脆弱性なし	Â
12.2SXE	脆弱性なし	Â
12.2SXF	脆弱性なし	Â
12.2SXH	脆弱性なし	Â
12.2SXI	脆弱性なし	Â
12.2SY	脆弱性なし	Â
12.2SZ	脆弱性なし	Â
12.2T	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.2TPC	Release prior to 12.2(8)TPC10d are vulnerable， releases 12.2(8)TPC10d and later are not vulnerable;	Â
12.2UZ	脆弱性なし	Â
12.2XA	脆弱性なし	Â
12.2XB	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.2XC	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.2XD	脆弱性なし	Â
12.2XE	脆弱性なし	Â

12.2XF	脆弱性なし	Â
12.2XG	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.2XH	脆弱性なし	Â
12.2XI	脆弱性なし	Â
12.2XJ	脆弱性なし	Â
12.2XK	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.2XL	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.2XM	脆弱性なし	Â
12.2XN	脆弱性なし	Â
12.2XNA	脆弱性なし	Â
12.2XO	脆弱性なし	Â
12.2XQ	脆弱性なし	Â
12.2XR	脆弱性なし	Â
12.2XS	脆弱性なし	Â
12.2XT	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.2XU	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.2XV	脆弱性なし	Â
12.2XW	脆弱性なし	Â
12.2YA	脆弱性なし	Â
12.2YB	脆弱性なし	Â
12.2YC	脆弱性なし	Â
12.2YD	脆弱性なし	Â
12.2YE	脆弱性なし	Â
12.2YF	脆弱性なし	Â
12.2YG	脆弱性なし	Â
12.2YH	脆弱性なし	Â
12.2YJ	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.2YK	脆弱性なし	Â
12.2YL	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.2YM	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.2YN	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.2YO	脆弱性あり; migrate to any release in 12.2SY	12.2(18)SXF15; 08-AUG-08 で利用可能
12.2YP	脆弱性なし	Â

12.2YQ	脆弱性なし	Â
12.2YR	脆弱性なし	Â
12.2YS	脆弱性なし	Â
12.2YT	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.2YU	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.2YV	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.2YW	脆弱性なし	Â
12.2YX	脆弱性なし	Â
12.2YY	脆弱性なし	Â
12.2YZ	脆弱性なし	Â
12.2ZA	脆弱性なし	Â
12.2ZB	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.2ZC	脆弱性なし	Â
12.2ZD	脆弱性あり; contact TAC	Â
12.2ZE	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.2ZF	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.2ZG	脆弱性あり; first fixed in 12.4T	12.4(19a) 12.4(19b) 12.4(20)T; 11-JUL-08 で利用可能
12.2ZH	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b) 12.4(20)T; 11-JUL-08 で利用可能
12.2ZJ	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.2ZL	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b) 12.4(20)T; 11-JUL-08 で利用可能
12.2ZP	脆弱性なし	Â
12.2ZU	脆弱性なし	Â
12.2ZY	脆弱性なし	Â
12.2ZYA	脆弱性なし	Â
Affected 12.3-Based Release	First Fixed Release (修正された最初のリリース)	**推奨リリース**

s		
12.3	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.3B	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.3BC	脆弱性なし	Â
12.3BW	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.3EU	脆弱性なし	Â
12.3JA	脆弱性なし	Â
12.3JEA	脆弱性なし	Â
12.3JEB	脆弱性なし	Â
12.3JEC	脆弱性なし	Â
12.3JK	脆弱性なし	Â
12.3JL	脆弱性なし	Â
12.3JX	脆弱性なし	Â
12.3T	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.3TPC	脆弱性あり; contact TAC	Â
12.3VA	脆弱性あり; contact TAC	Â
12.3XA	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b) 12.4(20)T; 11-JUL-08 で利用可能
12.3XB	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.3XC	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b) 12.4(20)T; 11-JUL-08 で利用可能
12.3XD	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.3XE	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b) 12.4(20)T; 11-JUL-08 で利用可能
12.3XF	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.3XG	脆弱性あり; first fixed in 12.4T	12.4(19a) 12.4(19b) 12.4(20)T; 11-JUL-08 で利用可能
12.3XH	脆弱性あり; first fixed in 12.4	12.4(19a)

		12.4(19b)
12.3XI	脆弱性あり; contact TAC	Â
12.3XJ	脆弱性あり; first fixed in 12.3YX	12.3(14)YX12 12.4(20)T; 11-JUL-08 で利用可能
12.3XK	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.3XQ	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.3XR	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b) 12.4(20)T; 11-JUL-08 で利用可能
12.3XS	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b)
12.3XU	脆弱性なし	Â
12.3XW	脆弱性あり; first fixed in 12.3YX	12.3(14)YX12 12.4(20)T; 11-JUL-08 で利用可能
12.3XY	脆弱性なし	Â
12.3YA	脆弱性あり; first fixed in 12.4	12.4(19a) 12.4(19b) 12.4(20)T; 11-JUL-08 で利用可能
12.3YD	脆弱性あり; first fixed in 12.4T	12.4(20)T; 11-JUL-08 で利用可能
12.3YF	脆弱性あり; first fixed in 12.3YX	12.3(14)YX12 12.4(20)T; 11-JUL-08 で利用可能
12.3YG	脆弱性あり; first fixed in 12.4T	12.4(20)T; 11-JUL-08 で利用可能
12.3YH	脆弱性あり; first fixed in 12.4T	12.4(20)T; 11-JUL-08 で利用可能
12.3YI	脆弱性あり; first fixed in 12.4T	12.4(20)T; 11-JUL-08 で利用可能
12.3YJ	脆弱性なし	Â
12.3YK	脆弱性あり; first fixed in 12.4T	12.4(20)T;

		11-JUL-08 で利用可能
12.3YM	Release prior to 12.3(14)YM12 are vulnerable， releases 12.3(14)YM12 and later are not vulnerable;	12.3(14)YM12
12.3YQ	脆弱性なし	Â
12.3YS	脆弱性あり; first fixed in 12.4T	12.4(20)T; 11-JUL-08 で利用可能
12.3YT	脆弱性あり; first fixed in 12.4T	12.4(20)T; 11-JUL-08 で利用可能
12.3YU	脆弱性あり; first fixed in 12.4XB	Â
12.3YX	12.3(14)YX12	12.3(14)YX12
12.3YZ	脆弱性あり; contact TAC	Â
Affected 12.4-Based Releases	**First Fixed Release (修正された最初のリリース)**	**推奨リリース**
12.4	12.4(18b) 12.4(19a) 12.4(19b) 12.4(21)	12.4(19a) 12.4(19b)
12.4JA	脆弱性なし	Â
12.4JK	脆弱性なし	Â
12.4JMA	脆弱性なし	Â
12.4JMB	脆弱性なし	Â
12.4JMC	脆弱性なし	Â
12.4JX	脆弱性なし	Â
12.4MD	12.4(15)MD	12.4(15)MD
12.4MR	12.4(19)MR	12.4(19)MR
12.4SW	脆弱性あり; contact TAC	Â
12.4T	12.4(15)T6 12.4(20)T; 11-JUL-08 で利用可能	12.4(20)T; 11-JUL-08 で利用可能
12.4XA	脆弱性あり; first fixed in 12.4T	12.4(20)T; 11-JUL-08 で利用可能
12.4XB	12.4(2)XB10	Â
12.4XC	脆弱性あり; contact TAC	Â
12.4XD	12.4(4)XD11; 31-JUL-08 で利用可能	12.4(20)T; 11-JUL-08

		で利用可能
12.4XE	脆弱性あり; first fixed in 12.4T	12.4(20)T; 11-JUL-08 で利用可能
12.4XF	脆弱性なし	Â
12.4XG	脆弱性なし	Â
12.4XJ	脆弱性あり; first fixed in 12.4T	12.4(20)T; 11-JUL-08 で利用可能
12.4XK	脆弱性なし	Â
12.4XL	12.4(15)XL2	12.4(15)XL2
12.4XM	12.4(15)XM1	12.4(15)XM1
12.4XN	脆弱性あり; contact TAC	Â
12.4XQ	脆弱性あり; contact TAC	Â
12.4XT	脆弱性あり; contact TAC	Â
12.4XV	脆弱性あり; contact TAC	Â
12.4XW	12.4(11)XW8	12.4(11)XW6
12.4XY	12.4(15)XY3	Â
12.4XZ	脆弱性あり; first fixed in 12.4T	12.4(20)T; 11-JUL-08 で利用可能

Cisco Network Registrar

影響を受けたリリース トレイン	First Fixed Release（修正された最初のリリース）
Pre-6.1.x	ソフトウェアはサポート終了ステータスに達しました。 pre-6.1.x バージョンを実行している顧客は新しいバージョンにできるだけ早くアップグレードするように勧告されます。
6.1.x	6.2.4.1 へのアップグレード; 現在公開中
6.2.x	6.2.4.1; 現在公開中
6.3.x	6.3.1.5; 現在公開中
7.0.x	7.0.1; 利用可能 な 2008 年 9月末頃

Cisco Network Registrar ソフトウェアは http://www.cisco.com/pcgi-bin/Software/Tablebuild/tablebuild.pl/nr-eval?psrtdcat20e2 でダウンロード可能です

Cisco Application and Content Networking System（ACNS）ソフトウェア

この問題は今利用可能である Cisco ACNS ソフトウェアのバージョン 5.5.11.2 で解決されます。

Cisco ACNS 5.5 ソフトウェアは http://www.cisco.com/pcgi-bin/tablebuild.pl/acns55?psrtdcat20e2 でダウンロード可能です。

不正利用事例と公式発表

Cisco PSIRT はこのアドバイザリに記載される脆弱性の不正利用に気づいていません。 脆弱性の性質についての完全な技術的詳細は共用利用可能であり、Metasploit プロジェクトはこの脆弱性を不正利用できる 2 つのモジュールを送達しました。

不正侵入の毒する DNS キャッシュが新しくないが、ダン Kaminsky IOActive のセキュリティ研究者は最近成功するために不正侵入のもっと多分毒する DNS キャッシュを作る手法を示しました。 Cisco は彼の調査結果についてのベンダーを知らせるためにダン Kaminsky に感謝することを望みます。

Cisco IOSソフトウェアのための脆弱性情報が脆弱性の業界全体公開による http://www.cisco.com/go/psirt で記述されている Cisco IOSソフトウェアにアナウンスされたパブリケーション スケジュールのこの諮問外部で提供されていることに注目して下さい。

US-CERT によって公開されるマルチベンダ アドバイザリは http://www.kb.cert.org/vuls/id/800113 （"VU#800113 - 脆弱 な複数の DNS 実装中毒を」キャッシュするため）で利用できます。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080708-dns

改訂履歴

Revision 2.1	2008 9 月 09 日	Ciscoアプリケーションのための追加された Cisco バグ ID は「ポート アドレス変換考慮事項」セクションに PAT をするときこれらのデバイスは予想できる送信元ポート 割り当て ポリシーがあるかもしれないのでエンジン（ACE）モジュールおよび Cisco ACE アプライアンスを制御します。Cisco Network Registrar と Cisco Application and Content Networking System（ACNS）ソフトウェアのための更新済修正済みソフトウェア 情報および有効 日付。
Revision 2.0	2008-July-28	DNSサーバが PAT を行うネットワークデバイスの後ろに強調表示しある PAT を行うことができる PAT オペレーションのた

		めに必要とされるレイヤ4 書き直しを行うとき予想できる送信元ポート 割り当て ポリシーを使用するシスコ製品に情報および Cisco バグ ID を追加し、とき「ポート アドレス変換考慮事項」セクションを問題および危険性を提供するために。 Cisco Network Registrar のための更新済修正済みソフトウェア 有効 日付。
リビジョン 1.2	2008-July-25	「不正利用事例と公式発表」セクションを完全な技術的詳細およびエクスプロイトコードが共用利用可能であることを示すためにアップデートしました。 US-CERT 脆弱性に関する注記への追加されたリンク。
リビジョン 1.1	2008-July-22	CVSS スコア カルキュレータへの固定リンク。 Cisco Network Registrar のための修正済みソフトウェアの更新済表。 脆弱性の詳細の公の議論に気づいていることを述べて下さい。 ACNS ソフトウェアのための情報更新済アベイラビリティの。
リビジョン 1.0	2008-July-08	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。