Ciscoコンテンツサービススイッチ11000シリーズのDNSネガティブキャッシュにおける情報のDoS脆弱性

アドバイザリーID : cisco-sa-20030430-dns
初公開日 : 2003-04-30 08:00
バージョン 1.2 : Final
回避策 : No Workarounds available
Cisco バグ ID :

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コンテンツサービススイッチ(CSS)11000および11500シリーズスイッチは、エラーコードとStart of Authority(SOA)レコードなしで、特定のDomain Name Service（DNS；ドメインネームサービス）ネームサーバレコード要求に応答します。これは、一部のDNSネームサーバで負の方向にキャッシュされる可能性があり、CSSがホストする特定のドメイン名に対するサービス拒否攻撃の原因となります。この脆弱性の影響を受けるには、CSSデバイスでグローバルサーバロードバランシングが設定されている必要があります。CERT/CCはこの問題に関する脆弱性ノートを発行しました(VU#714121)。シスコは修正済みソフトウェアを提供しており、お客様には修正済みコードへのアップグレードをお勧めします。

CSSにおけるこの脆弱性は、Cisco Bug ID CSCdz62499およびCSCea36989として文書化されています。

このアドバイザリは、
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20030430-dnsで確認できます。

該当製品

脆弱性のある製品

CSS 11000および11500シリーズスイッチ（以前のArrowpoint）は、CSS 11050、CSS 11150、CSS 11800 11501、11503、および11506ハードウェアプラットフォームで構成されます。Cisco WebNSソフトウェアを実行する

WebNSソフトウェアリビジョンが稼働しているCSS 11000および11500シリーズスイッチは

、グローバルサーバロードバランシング（DNSロードバランシングとも呼ばれる）が設定されている場合にのみ、この脆弱性の影響を受けます。

使用しているCSS機器でグローバルサーバロードバランシングが設定されているかどうかを確認するには、dns-serverコマンドの設定を確認してください。このコマンドが存在しない場合、設定はこの問題に対して脆弱ではありません。

脆弱性を含んでいないことが確認された製品

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

一般に、インターネットで使用されているネームサービス(DNS)は、DNSサーバとクライアント間のクエリーにさまざまなレコードタイプを使用します。一般的なレコードタイプには、アドレスレコード（Aレコード）、ネームサーバーレコード（NSレコード）、メール交換（MXレコード）、Start of Authorityレコード（SOAレコード）、および標準名レコード（CNAMEレコード）があります。各レコードまたはクエリの種類には、キャッシュできる内容や他のクライアントが信頼できる内容など、さまざまな規則や形式が関連付けられています。

通常、クライアントはローカルサーバにクエリを送信し、そのローカルサーバはクライアントに対する応答を作成するために、そのクライアントに代わって他のサーバにクエリを送信します。ローカルサーバが応答を受信すると、今後の使用に備えて情報をキャッシュし、クライアントに応答します。

CSS 11000および11500シリーズスイッチは、権威DNSネームサーバとして機能し、DNS Aレコード要求にのみ応答します。グローバルサーバロードバランシング機能を介してDNS用に設定されたCSSが、サポートされていないレコードタイプに対するDNS要求またはクエリを受信した場合、CSSは、WebNSのバージョンに応じて、rcode 4「not implemented」またはrcode 3「NXDOMAIN」で応答します。NXDOMAIN応答コードを受信すると、クエリサーバは通常、その名前の他のレコードタイプの解決の試行を停止します。たとえば、AAAAクエリに対するNXDOMAIN応答によって、サーバがAクエリを送信しなくなることがありますが、実際にはAレコードが存在する可能性があります。NXDOMAIN応答を受信し、ネガティブキャッシュをサポートする一部のリゾルバは、ネガティブキャッシュされたエラー応答の期限が切れるまで同じ名前のAレコードを照会しません。この期限が切れると、長時間かかることがあります。

受信したDNSクエリーが正規のホスト名に対するものであるが、サポートされていないレコードタイプである場合、これらの否定応答はさまざまなプロキシまたはキャッシングネームサーバによってキャッシュされる可能性があり、他のクライアントが正規のホスト名に対してキャッシングネームサーバまたはプロキシを照会すると、一時的なサービスの停止が発生します。ネットワークサービスは物理的には影響を受けませんが、エンドユーザは名前解決に依存し、正しいDNS情報がないと、サービスが停止する可能性があります。

最初の修正はCisco Bug ID CSCdz62499で、応答がrcode 3からrcode 4に変更されています。この結果コードも負のキャッシュに保存されるため、Cisco Bug ID CSCea36989で完全な修正が正しく行われています。

CSSは、RFC 2308準拠のNODATAタイプ3応答を返すようになります。これは、rcode=NOERROR、answer=0、およびSOAなしの正式な応答です。この応答により、特定のクライアントは、サポートされていないレコードタイプのクエリを続行したり、負のキャッシュのエラーメッセージやNXDOMAIN応答を使用したりせずに、別のAレコードをクエリする必要があります。

回避策

この問題の回避策は、修復されたバージョンへのアップグレードがインストール可能になるまで、グローバルサーバロードバランシングを無効にして、該当するサーバとドメインのDNSレコードを、別の準拠するDNSサーバで設定することです。

修正済みソフトウェア

次の表に、この通知に記載された不具合の影響を受けるCSSソフトウェアリリースの概要と、対応する最初の修正済みリリースが利用可能になる予定日を示します。日程は暫定的なものであり、変更されることがあります。

リリースを選択する際には、次の定義に注意してください。

- メンテナンスリリースは、最も頻繁にテストされ、強く推奨されるリリースです。
- 暫定リリースは、メンテナンスリリースに比べてテストが大幅に少ないため、この不具合を修正する適切なリリースが他にない場合にのみ選択してください。

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。

該当するバージョン	修正済みバージョン	利用可能な予定日
5.00.1.05以前の5.00 • 5.00ビルド105 (ap0500105.adi-gz)	5.00.1.08S – 暫定ビルド • 5.00ビルド108s (ap0500108s.adi-gz)	2003年4月29日

	5.00.2.01 – メンテナンスリリース • 5.00ビルド201 (ap0500201.adi-gz)	2003年5月30日
5.01、5.02、および5.03	6.10へのアップグレード – メンテナンスリリース	2003年5月15日
7.10.1.02以前の7.10 • 7.10ビルド102 (sg0710102.adi-gz)	7.20.0.03：メンテナンスリリース • 7.20ビルド003 (sg0720002.adi-gz)	現在利用可能
	7.10.2.06：メンテナンスリリース • 7.10ビルド206 (sg0710206.adi-gz)	現在利用可能

注：上記の表の箇条書き項目は、ビルドIDとファイル名（同じビルドに対する以前の命名規則）に関する情報を提供します。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

この脆弱性は、CERTによってhttp://www.kb.cert.org/vuls/id/714121で公開されています。CERTは、この問題は新しいものではないと述べています。Cisco PSIRTでは、このアドバ

イザリに記載されている脆弱性の不正利用事例は確認しておりませんが、この問題の性質により、エクスプロイトに気づいたり、報告されたりすることはありません。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20030430-dns

改訂履歴

リビジョン 1.0	2003年 4月30日	初回公開リリース
リビジョン 1.1	2003年 5月1日	「ソフトウェアバージョンと修正」に説明を加えるために、代替のビルド識別子が追加されました。
リビジョン 1.2	2003年 5月23日	バージョン番号を明確にするため、表の「該当バージョン」列の内容を編集。

利用規約

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。