Ciscoコンテンツサービススイッチの脆弱性

アドバイザリーID : cisco-sa-20010131-arrowpoint-cli-fs
初公開日 : 2001-01-31 16:00
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 Content Services(CSS)スイッチ製品（Arrowpointとも呼ばれる）では、コマンドラインインターフェイス(CLI)へのアクセスが許可されると、2つのセキュリティ脆弱性が発生します。1つ目の脆弱性は、非特権ユーザによってスイッチが一時的なサービス拒否(DoS)状態に置かれる可能性があるものです。この脆弱性は、Cisco Bug ID CSCdt08730に記載されています。2番目の問題では、非特権ユーザがファイル名とファイルの内容を表示できます。この問題は、Cisco Bug ID CSCdt12748に記述されています。

このアドバイザリの全文は、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20010131-arrowpoint-cli-fsで参照できます。

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

Ciscoコンテンツサービススイッチは、この脆弱性グループの影響を受けます。CSSスイッチはArrowpoint製品とも呼ばれ、Cisco WebNSソフトウェアを実行します。

Cisco CSS 11050、CSS 11150、およびCSS 11800ハードウェアプラットフォームは、この脆弱性グループの影響を受けます。

他のシスコ製品は、この脆弱性グループの影響を受けません。

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

Cisco CSS11000は、管理アドレスを指定し、ユーザアカウントを定義することによって、ユーザにコマンドラインアクセスを許可するように設定する必要があります。非特権ユーザ（管理権限のない定義済みユーザアカウント）がコマンドラインアクセスを取得した後、ファイル名を必要とするコマンドを実行し、入力バッファの最大長であるファイル名を指定すると、スイッチがリブートし、システムチェックが開始されて、スイッチが通常の動作を最大5分間実行できなくなる場合があります。show script、clear script、show archive、clear archive、show log、およびclear logコマンドを使用すると、指定したファイル名が入力バッファの最大長である場合にCSSを再起動できます。Cisco Bug ID CSCdt08730。

コマンド・ライン・アクセスが制限されていない場合、非特権ユーザー（管理権限のない定義済ユーザー・アカウント）は、存在しないファイル名を要求することによってディレクトリ構造に関する情報を取得できます。また、非特権ユーザは、ターゲットファイルのディレクトリ構造がユーザに認識されている場合、ファイルの読み取りアクセス権を取得できます。Cisco Bug ID CSCdt12748（登録ユーザ専用）では、このファイルシステムの脆弱性について説明しています。

回避策

アクセスコントロールリスト(ACL)を適用して、Cisco CSSデバイスへのアクセスを制限したり、管理インターフェイスへの接続を制限するための追加のファイアウォールやアクセスリストを適用したりできます。アクセスコントロールリストはCisco CSSデバイスの仮想インターフェイスへのトラフィックにも影響するため、注意して適用する必要があります。アクセスリストの設定の詳細については、次の製品ドキュメントを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/webscale/css/bsccfggd/profiles.htm

http://www.cisco.com/univercd/cc/td/doc/product/webscale/css/advcfggd/sgacleql.htm

また、SSHを使用してデバイスへの管理トラフィックのスヌーピングを防止することも推奨されます。

Telnetサービスも無効にできます。コロケーション環境の多くのお客様にとって、これは実行可能なオプションではありませんが、この設定を実装する機能を持つ可能性のあるお客様のために、このセクションで説明しています。

<#root>

CS150(config)#

telnet access disabled

また、お客様ご自身のセキュリティポリシーに従って強力なパスワードを選択し、パスワードを頻繁に変更したり、スタッフ配置の変更が発生した場合には、お客様自身のセキュリティポリシーに従うことをお勧めします。

修正済みソフトウェア

CSCdt08730は、Cisco WebNSソフトウェアのリビジョン4.01(12s)およびリビジョン3.10(71s)で解決されています。ファイルシステムの情報開示の脆弱性は、リビジョン4.01(23s)およびリビジョン4.10(13s)で解決されています。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

このアドバイザリで説明されている脆弱性の公表や悪用に関する情報は Cisco PSIRT には寄せられていません。これらの脆弱性は、お客様のセキュリティ監査中にセキュリティコンサルティング会社によって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20010131-arrowpoint-cli-fs

改訂履歴

リビジョン1.2	2001年4月13日	「ソフトウェアバージョンと修正」セクションが、Cisco WebNSソフトウェアのリビジョン4.01(12s)およびリビジョン3.10(71s)でCSCdt08730が解決されました。ファイル・システムの情報漏洩の脆弱性は、修正される予定ですが、現在未解決です。暫定的な回避策が推奨されます。この通知は、脆弱性が解決された時点で更新されます。または、脆弱性が解決されるまで毎月更新されます」 次のようにします。 “CSCdt08730は、Cisco WebNSソフトウェアのリビジョン4.01(12s)とリビジョン

		3.10(71s)で解決されています。ファイルシステムの情報開示の脆弱性は、リビジョン4.01(23s)およびリビジョン4.10(13s)で解決されています。 この通知のステータスはINTERIMからFINALに変更され、この通知のステータスのセクションの下の言い回しは次のように変更されました。「これは暫定通知です。シスコでは、この通知のすべての内容が正確であることの保証はできませんが、可能な限りすべての事実を確認しています。シスコでは、ソフトウェアのアップデートに伴い、この通知のアップデートバージョンが発行されることを想定しています。シスコは2001年3月1日までにこの通知を更新します」 次のようにします。 「これは最終的な通知です。シスコでは、この通知のすべての内容が正確であることの保証はできませんが、可能な限りすべての事実を確認しています。シスコは、これらの事実に重大な変更がない限り、この通知のアップデート バージョンを発行する予定はありません。事実に重大な変更があった場合、シスコはこの通知を更新する可能性があります」
リビジョン1.1	2001年2月2日	次の文が変更されました。「Ciscoコンテンツサービス(CSS)スイッチ製品（Arrowpointとも呼ばれる）には、コマンドラインインターフェイス(CLI)へのアクセスが許可された後にいくつかのセキュリティ脆弱性があります。」 次のようにします。 「Cisco Content Services(CSS)スイッチ製品はArrowpointとも呼ばれ、コマンドラインインターフェイス(CLI)へのアクセスが

		許可されると、2つのセキュリティ脆弱性が存在します。」 「数個」を「二」に改めた
リビジョン1.0	2001年1月31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。