

Ciscoコンテンツサービススイッチのユーザアカウントの脆弱性

severity

アドバイザリーID : cisco-sa-20010404-arrowpoint-usr-accnt-bug
初公開日 : 2001-04-04 15:00
バージョン 1.0 : 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 (別名Arrowpoint) には、以前のリリースに存在するセキュリティ脆弱性により、非特権ユーザが特権レベルを昇格でき、該当するユニットでの設定機能が許可されます。この脆弱性は、有効なユーザアカウントからのみ実行できます。

この脆弱性を排除するため、シスコでは該当するすべてのプラットフォームでリビジョン 4.01B19sへの無償ソフトウェアアップグレードを提供しています。この不具合は、Cisco Bug ID CSCdt32570に記載されています。

このアドバイザリーは、

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20010404-arrowpoint-usr-accnt-bug>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

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の影響を受けます。他のシスコ製品はこの脆弱性の影響を受けません。

スイッチで4.01B19sよりも前のバージョンが稼働している場合は、この問題に該当するため、できるだけ早くアップグレードする必要があります。コマンドラインでversionと入力すると、ソフトウェアのバージョン番号を確認できます。

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

非特権ユーザは、一連のキーストロークを発行してデバッグモードに入り、そのモードから管理アクセスを取得できます。

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/bsscfcgd/profiles.htm>

<http://www.cisco.com/univercd/cc/td/doc/product/webScale/css/advfcfgd/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サービスを無効にすることもできます。これは、コロケーション環境の多くのお客様にとって実行可能なオプションではありませんが、このセクションでは、この設定を実装できる可能性のあるお客様のために説明しています。

```
<#root>
```

```
CS150(config)# telnet access disabled
```

修正済みソフトウェア

CSCdt32570は、Cisco WebNSソフトウェアのバージョン4.01B19sで解決されています。非特権ユーザはデバッグモードに入ることはできなくなりました。

推奨事項

```
$propertyAndFields.get("recommendations")
```

不正利用事例と公式発表

シスコでは、この通知の日付より前に、この脆弱性に関する公表や議論は行っておりません。シスコには、この脆弱性の悪意のあるエクスプロイトに関する報告はありません。この不具合は、シスコのテクニカルサポートスタッフによって特定され、報告されたものです。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20010404-arrowpoint-usr-accnt-bug>

改訂履歴

リビジョン 1.0	2001年4月4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、単独の転載や意識を施した場合、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。