# Cisco Small Business SRP500シリーズコマンドインジェクションの脆弱性

**Critical**

**アドバイザリーID :** cisco-sa-20111102-srp500

**初公開日 :** 2011-11-02 16:00

**バージョン 1.0 :** Final

**CVSSスコア :** 9.3

**回避策 :** No Workarounds available

**Cisco バグ ID :** CSCtr45124

CVE-2011-4005

**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 Small Business SRP500シリーズServices Readyプラットフォームには、オペレーティングシステムコマンドインジェクションの脆弱性が存在します。 この脆弱性は、 Services Ready Platform Configuration UtilityのWebインターフェ イスへのリモートセッションを介して不正利用される可能性があります。

シスコはこの脆弱性に対処するソフトウェアアップデートをリリースしています。

この脆弱性を軽減する回避策があります。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20111102-srp500 で公開されています。

## 該当製品

### 脆弱性のある製品

バージョン1.1.24より前のファームウェアを実行している場合、次の Cisco Small Business SRP520シリーズモデルが影響を受けます。

- Cisco SRP521W
- Cisco SRP526W
- Cisco SRP527W

バージョン1.2.1より前のファームウェアを実行している場合、次のCisco Small Business

SRP540シリーズモデルが影響を受けます。

- Cisco SRP541W
- Cisco SRP546W
- Cisco SRP547W

デバイスのファームウェアバージョンを表示するには、Services Ready Platform Configuration Utilityにログインし、[Status] > [Router] ページに移動して、SRPとそのファームウェアステータスに関する情報を表示します。 **Firmware Version**フィールドには、SRP500シリーズデバイスで現在実行されているファームウェアのバージョンが表示されます。

### 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

Cisco Small Business SRP500シリーズServices Readyプラットフォームは、柔軟でコスト効率の高い固定構成の顧客宅内機器(CPE)です。組み込みのインテリジェンスにより、サービスプロバイダーは必要に応じて、高品質なIP音声、データ、セキュリティ、およびワイヤレスサービスなど、収益を生み出す高度なサービスを小規模企業に対して作成、プロビジョニング、および導入できます。

該当するバージョンのファームウェアを実行しているCisco Small Business SRP500シリーズデバイスには、次の脆弱性が存在します。

**Cisco Small Business SRP500シリーズServices Readyプラットフォームにおけるコマンドインジェクションの脆弱性**

この脆弱性は、Cisco Bug ID CSCtr45124 ( 登録ユーザ専用)に記載されており、割り当てられています Common Vulnerabilities and Exposures(CVE)ID CVE-2011-4005。

この脆弱性を不正利用するには、リモート攻撃者が巧妙に細工されたリンクにアクセスするよう管理者を誘導するか、認証されたセッションを傍受して中間者攻撃を実行する必要があります。挿入されるオペレーティングシステムコマンドは、ルートユーザのコンテキストで実行されます。

## 回避策

次の緩和策は、この脆弱性の発現を制限するのに役立ちます。

- リモート管理の無効化

**注意：管理者**がWAN接続を介してデバイスを管理している場合は、リモート管理を無効にしないでください。この操作を行うと、デバイスへの管理接続が失われます。

リモート管理はデフォルトで有効になっています。管理者は、[Administration] > [Web Access Management] を選択して、この機能を無効にできます。[Remote Management]フィールドの設定を[Disabled]に変更します。

リモート管理を無効にすると、この脆弱性はLAN間ネットワークからのみ悪用されるため、エクスポージャが制限されます。

- リモート管理アクセスを特定のIPアドレスに制限する

リモート管理が必要な場合は、[すべてのIPアドレス(All IP Addresses)]のデフォルト設定ではなく、特定のIPアドレスのみによってアクセスできるようにデバイスを保護します。管理者は、[Administration] > [Web Access Management] を選択した後、[Allowed Remote IP Address]設定を変更して、指定したIPアドレスを持つデバイスだけがデバイスにアクセスできるようにすることができます。

# 修正済みソフトウェア

アップグレードを検討する場合は、 http://www.cisco.com/go/psirt と後続のアドバイザリも参照して、問題の解決状況と完全なアップグレード ソリューションを確認してください。

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。情報が明確でない場合は、Cisco Small Business Support Center(SBSC)または契約したメンテナンスプロバイダーに問い合せて支援を求めてください。

この脆弱性は、次のファームウェアバージョンで修正されています。

| 該当製品 | First Fixed Release ( 修正された最初のリリース ) |
|---|---|
| Cisco SRP521W | 1.1.24 |
| Cisco SRP526W | 1.1.24 |
| Cisco SRP527W | 1.1.24 |
| Cisco SRP541W | 1.2.1 |
| Cisco SRP546W | 1.2.1 |
| Cisco SRP547W | 1.2.1 |

最新のCisco Small Business SRP500 Series Services Ready Platformsファームウェアは、http://www.cisco.com/cisco/software/navigator.html?mdfid=282736194&i=rmからダウンロードできます。

## 不正利用事例と公式発表

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。この脆弱性は、2011年11月2日にカリフォルニア州サンノゼで開催された会議で実証されました。

この脆弱性は、ポーランドのSecuritum社のMichal Sajdak氏によってシスコに報告されました。

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20111102-srp500

## 改訂履歴

| | | |
|---|---|---|
| リビジョン 1.0 | 2011年11月2日 | 初回公開リリース |

## 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。