# ソフトウェアアドバイザリ通知

お客様各位

ご使用のリリースについて、次のソフトウェアの問題が見つかりました。このソフトウェアの使用に影響を及ぼす可能性があります。このソフトウェアアドバイザリ通知を参照して、お客様の環境に該当する問題かどうかを確認してください。説明されている問題が該当しなければ、このソフトウェアのダウンロードに進むことができます。

このソフトウェアに含まれる内容の詳細については、製品セレクタツールから入手可能なシスコソフトウェアのリリースノートを参照してください。このページから、関心のある製品を選択します。リリースノートは、製品ページの「一般情報」にあります。

| CSCvp77466 の該当ソフトウェアと代替ソリューション | | |
|---|---|---|
| **[ソフトウェア タイプ（Software Type）]** | **該当するソフトウェア Versions:** | **ソフトウェアソリューション 修正済みソフトウェアバージョン：** |
| Cisco Secure Workload<br><br>（旧称 Cisco Tetration） | 実行中のカーネルバージョンに基づきます。詳細については、「問題の説明」に記載されている OS ディストリビュータからのアドバイザリを参照してください。 | 「回避策」セクションの説明に従って、オペレーティングシステムにパッチを適用します。 |

## アドバイザリの理由

Linux カーネルの IPSet コードのバグにより、複数の IPSet コマンドを同時に発行した場合に Linux システムがパニック状態になることがあります。

## 該当するソフトウェア

この問題は、適用が有効になっているパッチ未適用のカーネルバージョンで実行されている Cisco Secure Workload（Cisco Tetration ブランドのバージョンを含む）の適用エージェントに影響します。詳細については、「問題の説明」に記載されているアドバイザリを参照してください。

## 問題の説明

Linux マシンでのエージェントによるポリシーの適用時または再適用時に、エージェントで複数の ipset コマンドが発行されます。管理者が「ipset list」または「ipset save」コマンドを同時に実行すると、カーネルの ip_set コードのバグが原因でカーネルがパニック状態になる可能性があります。

このバグについては、次の Linux バグで説明されているように、さまざまな Linux ディストリビューションで報告されています。

- https://access.redhat.com/solutions/3520061
- https://bugs.centos.org/view.php?id=13767
- https://bugs.launchpad.net/ubuntu/+source/linux/+bug/1793753

## 回避策

OS ベンダーに問い合わせ、推奨されるパッチをインストールして問題に対処します。
適用が有効になっている適用エージェントを実行しているパッチ未適用のホストでは、「ipset save」または「ipset list」コマンドは実行しないでください。

アップストリームのバグリファレンス：

- https://github.com/torvalds/linux/commit/596cf3fe5854fe2b1703b0466ed6bf9cfb83c91e
- https://github.com/torvalds/linux/commit/e5173418ac597cebe9f7a39adf10be470000b518

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。