

データ分類を使用しないセキュアアクセス DLPファイルサイズ規則は、テキストファイル のモニタイベントを生成しません

内容

問題

ファイルサイズ基準のみ（データ分類なし）で設定されたCisco Secure Access Web DLPポリシーは、.txtファイルのアップロードに対してはDLPモニタイベントを生成しませんが、同じポリシーが.xlsx、.png、および.pdfファイルなどの他のファイルタイプに対してはモニタイベントを正しくトリガーします。影響を受けるポリシーSenior Management Policy - Webは次のように設定されています。

- 1KBから49MBまでのカスタムファイルサイズを持つファイル制御
- データ分類基準なし
- モニタするアクション

テストにより、次のことが判明しました。

- Action = Monitorの場合、TXTファイルのアップロードはDLPイベントに表示されません。
- Action = Blockの場合、同じTXTファイルでDLPイベントが正しく生成されます。
- アクティビティログには、TXTファイルを含むすべてのファイルアップロードが表示されます。
- その他のファイル形式(PNG、PDF、XLSX)では、モニタアクションで期待どおりにDLPイベントが生成されます。

また、DLPルールでデータ分類が設定されていない場合、ログに記録されるDLPイベントの重大度は、設定されているルールの重大度の設定にかかわらず、常にMediumになります。

環境

- Cisco Secure Access (旧称Cisco Umbrella)
- DLP (データ損失防止) Webポリシー
- HTTPS復号化が有効なインターネットアクセスポリシー
- Webアプリケーション経由でファイルアップロードテストを実施

解決方法

この動作は文書化されていませんが、設計上は予期されています。ログのオーバーロードを防ぐために、モニタアクションでファイルサイズのための基準を使用する場合、text/plainなどのMIMEタイプはDLPモニタリングからバイパスされます。開発チームは、これは外部に文書化されていない意図的な動作であることを確認しました。

回避策のオプション

オプション1 (推奨) : データ分類の追加

Action = Monitorの状態を維持したまま、幅広いデータ分類基準をDLPルールに追加します。

これにより、以下が復元されます。

- TXTファイルのDLPイベント生成
- ルール設定に基づく適切な重大度の処理

オプション2 : アクションをブロックに変更

ルールのアクションを[モニタ]から[ブロック]に変更します。これにより、TXTファイルに対するDLPイベントが生成されますが、モニタリングのみの使用例には望ましくないブロッキングも実行されます。

ラボテストの結果

包括的なラボテストにより、動作パターンを確認しました。

テストシナリオ1：データ分類とファイルサイズ(1KB ~ 49MB)を含むDLPルール、アクション=ブロック

- PIIを含むTXTファイル：ブロックおよび記録されました
- PDFファイル：ブロックおよびログ
- PIIのないTXTファイル：許可（必要）
- PII付きPNG：許可（分類に基づいて指定）

テストシナリオ2：ファイルサイズのみ（データ分類なし）のDLPルール、アクション=ブロック

- すべてのファイルタイプ(TXT、PDF、PNG)：ブロックおよび記録
- ルールがLowに設定されているにもかかわらず、重大度がMediumと表示される

テストシナリオ3：ファイルサイズのみ（データ分類なし）のDLPルール、アクション=モニタ

- TXTファイル：許可されるがDLPイベントに記録されない
- PDFおよびPNGファイル：許可およびログインしたDLPイベント
- アクティビティログには、TXTファイルを含むすべてのアップロードが表示されます

原因

これは意図的な動作ですが、Cisco Secure Access DLPでのドキュメント化されていない動作です。過剰なログ生成を防ぐために、モニタアクションでファイルサイズのためのルールを使用する場合、システムはtext/plain MIMEタイプのDLPイベントロギングをバイパスします。動作はアクションに依存し、MIMEタイプ固有です。

- Monitor action with file size-only基準：ロギングからバイパスされたTXTファイル
- ブロックサイズのための条件を指定したブロックアクション：TXTファイルが正常に記録される
- データ分類が存在するすべてのアクション：TXTファイルが正常に記録される

この重大度の問題は、DLPイベントがコンテンツ対応モードで動作しているときに、ルール設定ではなくデータ分類メタデータから重大度を取得するために発生します。データ分類を使用しない場合、設定されているルールの重大度に関係なく、システムはデフォルトで「Medium」の重大度に設定されます。

関連コンテンツ

- [Cisco Secure Access DLPファイルサイズの設定](#)

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。