クラウド接続の損失時にユーザアクションをブロックするDLPフェールクローズ動作の設定

内容

問題

エンドポイントDLP(EDLP)モジュールをインストールしたユーザで、設定されたEDLPルールに含まれていないにもかかわらず、印刷とネットワークファイル共有へのコピーがブロックされていました。既存のEDLPルールはすべて、3人の特定ユーザのみを含むモニタモードで設定されていました。影響を受けるユーザは、EDLPの適用を意図していなかったにもかかわらず、印刷操作およびファイル共有コピー操作で予期しないブロックアクションを検出しました。

トラブルシューティング中、EDLPクラウド接続が利用できない場合にブロックが発生したことが確認されたため、フォールバックメカニズムとしてフェールクローズ動作が適用されました。このユーザは、EDLPクライアントがポリシー判定のためにクラウドサービスへの接続を確立していない期間中に、印刷およびネットワーク共有アクセスの拒否を受けました。

環境

- Cisco Endpoint DLPモジュールバージョン1.5.0.292
- Cisco Secure Access/Secure/Data Loss Preventionポータル管理
- MONITORモードで設定された複数のEDLPルール
- フェールクローズ動作が設定されたネットワーク共有チャネル
- クライアントネットワーク接続に影響するDNS解決の変更

解決方法

この問題を解決するには、EDLPのフェールクローズ動作と、クラウド接続が失われたときのアプリケーションを理解し、説明する必要がありました。

根本原因の分析

DARTバンドルとEDLPログの分析により、ネットワーク共有チャネルがフェールクローズとして設定されているために、EDLPが拒否フォールバックを適用したことが判明しました。ブロッキングインシデントが発生した時点では、クライアントネットワークのDNS解決が変更されたため、EDLPクラウド接続が利用できず、システムはクラウドサービスからポリシー判定を取得できませんでした。

フェールクローズ動作の説明

ユーザーのIDが特定のEDLPルールに含まれているかどうかに関係なく、EDLPモジュールがインストールされているため、ユーザーのシステムにフェールクローズポリシーが適用されました。フェールオープン/フェールクローズ状態は、DLPポリシー設定でプロビジョニングされるグローバル設定であり、チャネル設定はそのグローバル設定に基づいて適用されます。

接続の回復

この問題は、クライアントネットワークでDNSの安定性が回復すると自動的に解決され、EDLPクライアントはクラウドサービスへの接続を再確立できます。基盤となるネットワーク接続の問題が解決すれば、手動による介入は必要ありません。

フェールクローズ動作を引き起こす状態

次の条件がEDLPのフェールクローズ動作を引き起こす可能性があります。

- DNS解決の問題
- ネットワーク停止
- ネットワークの切り替え

- クライアントとクラウドサービス間のエンドツーエンド接続を妨げるあらゆる条件

原因

ブロック動作は、ネットワーク共有チャネルに対するEDLPのフェールクローズ設定が原因です。DNS解決の変更が原因でEDLPクライアントがクラウドサービスへの接続を失うと、ポリシー判定を取得できないため、設定されたフェールクローズ動作がセキュリティフォールバックメカニズムとして適用されます。フェールクローズの設定は、クラウド接続が使用できないときにEDLPモジュールがインストールされたすべてのシステムにグローバルに適用されるため、ユーザがEDLPルールに明示的に含まれているかどうかにかかわらず、この問題が発生しました。

関連コンテンツ

- シスコのテクニカルサポートとダウンロード

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。