DCE TCP インスペクタ

- DCE TCP インスペクタの概要 （1 ページ）
- DCE TCP インスペクタのパラメータ （3 ページ）
- DCE TCP インスペクタのルール （5 ページ）
- DCE インスペクタの侵入ルールのオプション （6 ページ）

DCE TCP インスペクタの概要

タイプ	インスペクタ（サービス）
使用方法	検査
インスタンス タイプ	マルチトン
その他のインスペクタが必要	なし
有効	`true`

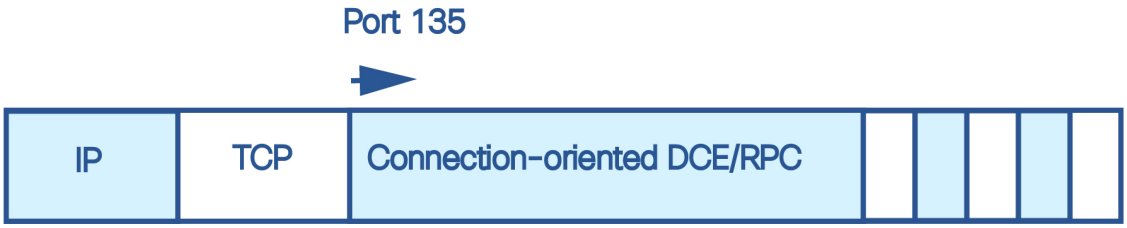
DCE/RPC プロトコルにより、別々のネットワーク ホスト上のプロセスが、同一ホストに配置されている場合と同様に通信できます。通常、このようなプロセス間通信はホスト間で TCP を介して転送されます。TCP 転送では、DCE/RPC が Windows Server Message Block（SMB）プロトコルまたは Samba でさらにカプセル化されることがあります。Samba は、Windows や UNIX または Linux のオペレーティングシステムから構成される混合環境でプロセス間通信に使用されるオープンソースの SMB 実装です。

ほとんどの DCE/RPC エクスプロイトは、DCE/RPC サーバ（ネットワーク上の Windows または Samba が稼働している任意のホスト）を対象とした DCE/RPC クライアント要求で発生します。またエクスプロイトはサーバ応答でも発生することがあります。

IP によりすべての DCE/RPC トランスポートがカプセル化されます。TCP は、すべてのコネクション型 DCE/RPC を伝送します。DCE TCP インスペクタは、コネクション型の DCE/RPC を検出し、プロトコル固有の特性（ヘッダー長やデータ フラグメントの順序など）を使用して次のことを行います。

- TCP トランスポートでカプセル化された DCE/RPC 要求を検出します。これには、RPC over HTTP バージョン 1 を使用して TCP で転送される DCE/RPC も含まれます。
- DCE/RPC データストリームを分析し、DCE/RPC トラフィック内の異常な動作と回避技術を検出します。
- DCE/RPC を最適化します。
- ルールエンジンで処理できるように DCE/RPC トラフィックを正規化します。

次の図に、DCE TCP インスペクタが TCP トランスポートのトラフィックの処理を開始するポイントを示します。



ウェルノウン TCP ポート 135 は、TCP トランスポートの DCE/RPC トラフィックを特定します。この図には RPC over HTTP は含まれていません。RPC over HTTP の場合、コネクション型 DCE/RPC は、図に示すように、HTTP を介した初期設定シーケンスの後、TCP 経由で直接伝送されます。

ターゲットベースのポリシー

Windows および Samba の DCE/RPC の実装は大きく異なります。たとえば、Windows のすべてのバージョンは、DCE/RPC トラフィックの最適化時に最初のフラグメントの DCE/RPC コンテキスト ID を使用しますが、Samba のすべてのバージョンは、最後のフラグメントのコンテキスト ID を使用します。また、特定の関数呼び出しを識別するために、Windows Vista では最初のフラグメントの opnum（操作番号）ヘッダーフィールドを使用しますが、Samba とその他のすべてのバージョンの Windows では最後のフラグメントの opnum フィールドを使用します。

そのため、`dce_tcp` インスペクタはターゲットベースのアプローチを使用します。`dce_tcp` インスペクタインスタンスを設定すると、`policy` パラメータは特定の DCE/RPC TCP プロトコルの実装を指定します。これをホスト情報と組み合わせることで、デフォルトのターゲットベースのサーバーポリシーが確立されます。必要に応じて、他のホストおよび DCE/RPC TCP の実装を対象とする追加のインスペクタを設定できます。デフォルトのターゲットベースのサーバーポリシーで指定されている DCE/RPC TCP の実装は、別の `dce_tcp` インスペクタインスタンスの対象になっていないすべてのホストに適用されます。

DCE TCP インスペクタが `policy` パラメータを使用してターゲットにできる DCE/RPC 実装は次のとおりです。

- WinXP（デフォルト）
- Win2000
- WinVista

- Win2003
- Win2008
- Win7
- Samba
- Samba-3.0.37
- Samba-3.0.22
- Samba-3.0.20

最適化

DCE TCP インスペクタでは、フラグメント化されたデータパケットを検出エンジンに送信する前に再設定することができます。この機能は、インラインモードで、完全な最適化が実行される前の検査プロセスの早い段階でエクスプロイトをキャッチしたり、フラグメント化を利用してそれ自体を隠すエクスプロイトをキャッチしたりするのに役立ちます。最適化を無効にすると、多数の誤検知が発生する可能性があることに注意してください。

DCE TCP インスペクタのパラメータ

DCE TCP ポートの設定

`binder` インスペクタは、DCE TCP ポートの設定を定義します。詳細については、『バインダインスペクタの概要』を参照してください。

例：

```
[
   {
        "when": {
            "role": "any",
            "proto": "tcp",
            "service": "dcerpc",
            "ports": ""
        },
        "use": {
            "type": "dce_tcp"
        }
    }
]
```

max_frag_len

最適化のために許可される最大フラグメント長をバイト単位で指定します。より大きなフラグメントを処理する場合、インスペクタは、最適化する前にパケットコンテンツに対して指定されたサイズに考慮します。

（注） このパラメータで指定する値は、確実に検出するためにルールでデータを調べる必要がある深さ以上にする必要があります。すべてのデータの検出が確実に行われるようにするには、デフォルト値を使用します。

型：整数

有効な範囲：1514 ～ 65535

デフォルト値：65535

disable_defrag

フラグメント化された DCE/RPC トラフィックを最適化するかどうかを指定します。このパラメータが true の場合、インスペクタは引き続き異常を検出して DCE/RPC データをルールエンジンに送信しますが、フラグメント化された DCE/RPC データでのエクスプロイトを見落とすリスクがあります。

このパラメータには、トラフィックを最適化しないという柔軟性があり、処理を高速化できますが、ほとんどの DCE/RPC エクスプロイトでは、フラグメント化を利用してエクスプロイトを隠ぺいする試行が行われます。このパラメータを有効にすると、既知のエクスプロイトのほとんどがバイパスされ、誤検知が大量に発生します。

型：ブール値

有効な値：true、false

デフォルト値：false

limit_alerts

DCE アラートをフローごとの署名ごとに最大 1 つに制限するかどうかを指定します。

型：ブール値

有効な値：true、false

デフォルト値：true

reassemble_threshold

リアセンブルされたパケットをルールエンジンに送信する前にキューに入れるには、DCE/RPC の最適化と最適化バッファの最小バイト数を指定します。このパラメータは、完全な最適化が実行される前の早い段階でエクスプロイトを検出する可能性があるため、インラインモードで役立ちます。

低い値を指定すると、早期検出の可能性が高くなりますが、パフォーマンスに悪影響を及ぼす可能性があります。このパラメータを有効にした場合は、パフォーマンスへの影響をテストする必要があります。

値 0 は、リアセンブルを無効にします。

型：整数

有効な範囲：0 ～ 65535

デフォルト値：0

policy

モニタ対象のネットワークセグメント上のターゲットホスト（複数可）が使用する Windows または Samba の DCE/RPC の実装を指定します。

型：列挙体

有効な値：Win2000、WinXP、WinVista、Win2003、Win2008、Win7、Samba、Samba-3.0.37、Samba-3.0.22、Samba-3.0.20 から選択した文字列

デフォルト値：WinXP

DCE TCP インスペクタのルール

dce_tcp インスペクタのルールを有効にし、イベントを生成し、インライン展開では、違反パケットをドロップします。。

表 *1 : DCE TCP* インスペクタのルール

GID:SID	ルール メッセージ
133:27	コネクション型 DCE/RPC：無効なメジャーバージョン（connection oriented DCE/RPC - invalid major version）
133:28	コネクション型 DCE/RPC：無効なマイナーバージョン（connection oriented DCE/RPC - invalid minor version）
133:29	コネクション型 DCE/RPC：無効な PDU タイプ（connection-oriented DCE/RPC - invalid PDU type）
133:30	コネクション型 DCE/RPC：フラグメント長がヘッダーサイズ未満（connection-oriented DCE/RPC - fragment length less than header size）
133:31	コネクション型 DCE/RPC：残りのフラグメント帳が必要なサイズ未満（connection-oriented DCE/RPC - remaining fragment length less than size needed）
133:32	コネクション型 DCE/RPC：コンテキスト項目が指定されていない（connection-oriented DCE/RPC - no context items specified）
133:33	コネクション型 DCE/RPC：転送シンタックスが指定されていない（connection-oriented DCE/RPC -no transfer syntaxes specified）

GID:SID	ルール メッセージ
133:34	コネクション型DCE/RPC：最後のフラグメント以外のフラグメント長がクライアントのネゴシエートされた最大フラグメント送信サイズ未満（connection-oriented DCE/RPC - fragment length on non-last fragment less than maximum negotiated fragment transmit size for client）
133:35	コネクション型DCE/RPC：フラグメント長がネゴシエートされた最大フラグメント送信サイズを超えている（connection-oriented DCE/RPC - fragment length greater than maximum negotiated fragment transmit size）
133:36	コネクション型DCE/RPC：バインドとは異なるコンテキストのバイト順序を変更する（connection-oriented DCE/RPC - alter context byte order different from bind）
133:37	コネクション型 DCE/RPC：最初/最後のフラグメント以外の呼び出し ID がフラグメント化された要求に対して確立された呼び出し ID と異なる（call id of non first/last fragment different from call id established for fragmented request）
133:38	コネクション型 DCE/RPC：最初/最後のフラグメント以外の opnum がフラグメント化された要求に対して確立された opnum とは異なる（connection-oriented DCE/RPC - opnum of non first/last fragment different from opnum established for fragmented request）
133:39	コネクション型 DCE/RPC：最初/最後のフラグメント以外のコンテキスト ID がフラグメント化された要求に対して確立されたコンテキスト ID とは異なる（connection-oriented DCE/RPC - context id of non first/last fragment different from context id established for fragmented request）

DCE インスペクタの侵入ルールのオプション

dce_iface

次のコンマ区切りの要素を指定します。

- サービスインターフェイスの UUID。
- インターフェイスのバージョン（オプション）。デフォルト設定は、どのバージョンにも一致します。
- ルールが要求内のいずれかのフラグメントに一致する必要があるかどうかのインジケータ（オプション）。デフォルト設定は、最初のフラグメントのみに一致します。

DCE/RPC プロトコルでは、クライアントはサービスを呼び出す前にサービスにバインドする必要があります。クライアントは、バインド要求をサーバーに送信するときに、バインド先の1つ以上のサービスインターフェイスを指定できます。各インターフェイスはUUIDで表され、

各インターフェイスの UUID は一意のインデックス（またはコンテキスト ID）とペアになっており、このインデックスを使用して、クライアントが呼び出しているサービスを今後の要求で参照できます。サーバーは、有効なものとして受け入れるインターフェイス UUID で応答し、クライアントがそれらのサービスに要求を行うことを許可します。クライアントが要求を行うと、コンテキスト ID が指定されるため、サーバーはクライアントが要求を行っているサービスを認識します。

dce_iface ルールオプションを使用すると、ルールは、クライアントが特定のインターフェイス UUID にバインドされているかどうかと、このクライアント要求がそのインターフェイスへの要求を行っているかどうかをインスペクタに問い合わせることができます。これにより、インスペクタがバインド UUID を要求で使用されるコンテキスト ID に関連付けることができるため、複数のサービスが正常にバインドされている場合の誤検知を排除できます。

dce_iface オプションは、インスペクタでのコネクション型の DCE/RPC に対するサーバーの Bind Ack 応答と Alter Context 応答だけでなく、クライアントの Bind 要求と Alter Context 要求の追跡が必要です。Bind および Alter Context 要求ごとに、クライアントは、インターフェイスを参照するために DCE/RPC セッション中に使用される各インターフェイス UUID のハンドル（またはコンテキスト ID）とともに、インターフェイス UUID のリストを指定します。サーバー応答は、クライアントが要求を行うことを許可するインターフェイスを示します。これは、特定のインターフェイスにバインドするクライアントの要求を受け入れるか拒否します。この追跡は、要求が処理されるときに、要求で使用されるコンテキスト ID を、それがハンドルであるインターフェイス UUID と関連付けることができるようにするために必要です。

dce_iface ルールオプションは、次の場合に一致します。

- 指定したインターフェイス UUID が DCE/RPC 要求のインターフェイス UUID（コンテキスト ID によって参照される）と一致する

および

- version 引数が指定されていないか、または version 引数が指定されていて、DCE/RPC 要求のインターフェイス UUID と一致する

および

- any_frag 引数が指定されているか、any_frag 引数がなく、dce_iface オプションが最初の要求フラグメントの UUID とバージョン基準に一致する

例：

```
dce_iface:4b324fc8-1670-01d3-1278-5a47bf6ee188;
dce_iface:4b324fc8-1670-01d3-1278-5a47bf6ee188, <2;
dce_iface:4b324fc8-1670-01d3-1278-5a47bf6ee188,any_frag;
dce_iface:4b324fc8-1670-01d3-1278-5a47bf6ee188, =1, any_frag;
```

dce_iface.uuid

DCE/RPC 要求では、UUID 番号がビッグエンディアンまたはリトルエンディアンのどちらで表されるかを指定できます。要求でのインターフェイス UUID の表現は、要求で指定したエンディアンに応じて異なります。dce_rpc インスペクタは UUID を正規化します。つまり、

dce_iface ルールオプションの UUID の指定は、要求のエンディアンに関係なく、同じように記述する必要があります。

たとえば、リトルエンディアンのバインド要求は、次のように UUID を表します。

```
|f8 91 7b 5a 00 ff d0 11 a9 b2 00 c0 4f b6 e6 fc|
```

ビッグエンディアンのバインド要求は、次のように同じ UUID を表します。

```
|5a 7b 91 f8 ff 00 11 d0 a9 b2 00 c0 4f b6 e6 fc|
```

dce_iface オプションを使用する Snort 3 ルールでは、要求のエンディアンに関係なく、ビッグエンディアン順を使用して UUID を文字列で表す必要があります。

```
5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc
```

型：文字列

シンタックス：`dce_iface: <UUID>;`

有効な値：*UUID* は 32 の 16 進数で、ハイフンで区切られた 5 つの グループ（xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx の形式）で表示されます。

例：`dce_iface: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc;`

dce_iface.version

サービスインターフェイスには、それに関連付けられたバージョンがあります。インターフェイスの一部のバージョンは、特定のエクスプロイトに対して脆弱ではない場合があります。そのため、dce_iface オプションで 1 つ以上のバージョン番号を指定して、特定のエクスプロイトを確認する必要があるかどうかを特定できます。

型：間隔

シンタックス：`dce_iface: <range_operator><positive integer>;` または `dce_iface: <positive integer><range_operator><positive integer>;`

有効な値：1 つ以上の一連の正のバージョン番号と、表 2 : 範囲の形式で指定されている range_operator の1 つ。

例：`dce_iface: =6;`

dce_iface.any_frag

DCE/RPC 要求は、1 つ以上のフラグメントに分割できます。DCE/RPC ヘッダーにフラグが設定されて現在のフラグメントが要求の最初のフラグメントか、中間のフラグメントか、または最後のフラグメントであるかを示します。DCE/RPC 要求内のデータの確認の多くは、DCE/RPC 要求が最初のフラグメント（または完全な要求）である場合にのみ関連します。したがって、最初のフラグメントに続くフラグメントには、DCE/RPC 要求のより深いデータが含まれます。たとえば、要求の最初の 5 バイト（長さフィールドなど）内のデータを検索するルールでは、最初のフラグメント以外のフラグメントで誤ったデータを検出します。後続のフラグメントの開始は、要求の開始からある程度の長さでオフセットされます。これは、フラグメント化された DCE/RPC トラフィックの誤検知の原因となる可能性があります。

そのため、デフォルトでは、DCE_RPC インスペクタは要求の最初のフラグメントのみを照合します。インスペクタが一致の要求内のすべてのフラグメントを調べるようにするには、dce_iface ルールオプションに any_frag を追加します。最適化された DCE/RPC 要求は完全な要求と見なされることに注意してください。

シンタックス：dec_iface: any_frag;

例：dce_iface: any_frag;

dce_opnum

DCE RPC 操作番号、操作番号の範囲、または操作番号のリストと照合します。このオプションは、インターフェイスに対して実行できる1つ以上の特定の関数呼び出しを表します。クライアントが特定のサービスインターフェイスにバインドして要求を行った後、ルールは、クライアントがサービスに対して行っている関数呼び出しを特定して、関数呼び出し内に存在する可能性のあるエクスプロイトを確認する必要があります。関数呼び出しは、操作番号（opnums）の二重引用符で囲まれたリストとして指定されます。

型：文字列

シンタックス：dce_opnum: <opnum_list>;

opnum_list は次のいずれかです。

- 単一の整数。
- コンマ区切りの整数のリスト。
- 範囲内の最小数と最大数をハイフンで区切って指定した整数の範囲。
- 上記の組み合わせ。

有効な値：DCE/RPC 要求の opnum のリスト。

例：

```
dce_opnum: "15";
dce_opnum: "15-18";
dce_opnum: "15, 18-20";
dce_opnum: "15, 17, 20-22";
```

dce_stub_data

このオプションは、先行するルールオプションに関係なく、DCE/RPC スタブデータの先頭に検出カーソル（ルール処理でパケットペイロードを通過させるために使用）を配置します。このオプションは、DCE/RPC スタブデータが存在する場合に一致します。

シンタックス：dce_stub_data;

例：dce_stub_data;

表 *2:* 範囲の形式

範囲の形式	演算子	説明
operator i		
	<	より少ない
	>	右辺と比較して大きい
	=	等しい
	≠	等しくない
	≤	以下
	≥	以上
j operator k		
	<>	j よりも大きく、k よりも小さい
	<=>	j 以上で k 以下

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。