SMTP インスペクタ

SMTP 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	`stream_tcp`
有効	`true`

Simple Mail Transfer Protcocol（SMTP）を使用すると、メールクライアントはメールサーバーにメッセージを送信できます。SMTP は、メッセージを受信者に配信するコマンドを発行します。SMTP サーバーは、安全でないセッションには TCP ポート 25 を使用し、SSL/TLS を介した SMTP には TCP ポート 587 を使用します。

`smtp` インスペクタは、SMTP トラフィックを検出し、SMTP コマンドと応答を分析します。

`smtp`インスペクタは、SMTP メッセージのコマンド、ヘッダー、および本文のセクションを識別し、Multi-purpose Internet Mail Extension（MIME）添付ファイルを抽出して復号化します。MIME 添付ファイルには、複数の添付ファイルや複数のパケットにまたがる大きな添付ファイルが含まれる場合があります。

`smtp` インスペクタは、SMTP メッセージを識別し、Snort の許可リストに追加します。有効にすると、侵入ルールは異常な SMTP トラフィックに関するイベントを生成します。

`smtp` インスペクタを次のように設定できます。

- セッションで生成されたすべてのイベントとともに、送信者の電子メール ID、受信者の電子メール ID、電子メールのヘッダー、および添付ファイルのファイル名をログに記録する。
- 余分な余白文字を削除して、SMTP コマンド ラインを正規化する。smtp インスペクタでスペース（ASCII 0x20）またはタブ（ASCII 0x09）文字を正規化する。
- TLS で暗号化されたトラフィックを無視してパフォーマンスを向上させる。
- プレーンテキストの電子メールデータを無視してパフォーマンスを向上させる。

SMTP インスペクタを設定するためのベストプラクティス

RFC 2821 のガイドラインに従って、smtp インスペクタのコア設定パラメータを設定することをお勧めします。

- max_command_line_len：512 文字
- max_header_line_len：1024 文字
- max_response_line_len：512 文字

SMTP インスペクタのパラメータ

SMTP サービスの設定

binder インスペクタは、SMTP サービス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": {
            "service": "smtp",
            "role": any
        },
        "use": {
            "type": "smtp"
        }
    }
]
```

alt_max_command_line_len[]

SMTP コマンドの配列と、コマンドの代替の最大行長を指定します。代替最大行長は、SMTP コマンドの max_command_line_len の値をオーバーライドします。このパラメータのイベントを生成するには、ルール 124:4 を有効にします。

型：配列

例：

```
{
    "alt_max_command_line_len": [
        {
            "command": "AUTH",
            "length": 240
        }
    ]
}
```

alt_max_command_line_len[].command

コマンド ストリングを指定します。

型：文字列

有効な値：SMTP コマンド

デフォルト値：「表 1 : SMTP コマンドとデフォルトの代替コマンド長」を参照してください。

alt_max_command_line_len[].length

代替の最大コマンドライン長を指定します。コマンドのコマンドライン長の検出を無効にするには、`0` を指定します。

型：整数

有効な範囲：`0` 〜 `4,294,967,295 (max32)`

デフォルト値：「表 1 : SMTP コマンドとデフォルトの代替コマンド長」を参照してください。

表 *1 : SMTP* コマンドとデフォルトの代替コマンド長

コマンド	長さ
ATRN	255
AUTH	246
BDAT	255
DATA	246
DEBUG	255
EHLO	500
EMAL	255
ESAM	255
ESND	255
ESOM	255

コマンド	長さ
ETRN	500
EVFY	255
EXPN	255
HELO	500
HELP	500
IDENT	255
MAIL	260
NOOP	255
ONEX	246
QUEU	246
QUIT	246
RCPT	300
RSET	255
SAML	246
SEND	246
SIZE	255
SOML	246
STARTTLS	246
TICK	246
TIME	246
TURN	246
TURNME	246
VERB	246
VRFY	255
XADR	246
XAUTH	246
XCIR	246
XEXCH50	246

コマンド	長さ
X-EXPS	246
XGEN	246
XLICENSE	246
X-LINK2STATE	246
XQUE	246
XSTA	246
XTRN	246
XUSR	246

auth_cmds

認証交換を開始するSMTPコマンドのリストを指定します。複数のSMTPコマンドはスペースで区切ります。

型：文字列

有効な値：SMTP 認証交換開始コマンド

デフォルト値：`AUTH XAUTH X-EXPS`

b64_decode_depth

各 Base64 エンコード MIME 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。65535 未満の整数を指定するか、または 0 を指定して復号化を無効にすることができます。復号化するバイト数に制限を設定しない場合は、-1 を指定します。

ルール 124:10 を有効にして、このパラメーターのイベントを生成し、インライン展開で、デコードが失敗したときに問題のあるパケットをドロップすることができます。

型：整数

有効な範囲：`-1` 〜 `65535`

デフォルト値：`-1`

binary_data_cmds

データの送信を開始し、コマンドの後に長さの値（オクテット単位）を使用して送信するデータの量を示すSMTPコマンドのリストを指定します。複数のSMTPコマンドはスペースで区切ります。

型：文字列

有効な値：データ長引数を使用する有効な SMTP データ送信開始コマンド

デフォルト値：`BDATA XEXCH50`

bitenc_decode_depth

バイトの最大数を指定し、エンコードされていない各MIME電子メールの添付ファイルから抽出します。65535 未満の整数を指定するか、または 0 を指定して、エンコードされていない MIME添付ファイルの抽出を無効にすることができます。抽出するバイト数に制限を設定しない場合は、-1 を指定します。これらの添付ファイルのタイプには、7 ビット、8 ビット、バイナリ、ならびにプレーンテキスト、JPEG イメージと PNG イメージ、および MP4 ファイルなど、マルチパートのコンテンツタイプが含まれます。

型：整数

有効な範囲：`-1` 〜 `65535`

デフォルト値：`-1`

data_cmds

データの送信を開始し、データの末尾のデリミタ（<CRLF>.<CRLF>）を使用する SMTP コマンドのリストを指定します。

型：文字列

有効な値：データの末尾のデリミタを使用する SMTP データ送信開始コマンド。

デフォルト値：`DATA`

decompress_pdf

MIME 添付ファイルの `application/pdf` （PDF） ファイルを圧縮解除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：`false`

decompress_swf

MIME 添付ファイルの `application/vnd.adobe.flash-movie` （SWF）の圧縮を解除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：`false`

decompress_vba

MIME 添付ファイルの Microsoft Office Visual Basic for Applications のマクロファイルの圧縮を解除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：`false`

decompress_zip

MIME 添付ファイルのアプリケーション/zip（ZIP）ファイルを解凍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：`false`

email_hdrs_log_depth

SMTP データから抽出する電子メールヘッダーのバイト数を指定します。電子メールヘッダーの抽出を無効にするには、0 を指定します。

型：整数

有効な範囲：`0` 〜 `20480`

デフォルト値：`1464`

ignore_data

電子メールデータセクションを復号化するかどうかを指定します（MIME 電子メールヘッダーを除く）。

型：ブール値

有効な値：`true`、`false`

デフォルト値：`false`

ignore_tls_data

TLS で暗号化されたデータを復号化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：`false`

log_email_hdrs

SMTP 電子メールヘッダーとセッションで生成されたすべてのイベントを復号化してログに記録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：`false`

log_filename

MIME 本文内の Content-Disposition ヘッダーから抽出された MIME 添付ファイル名とセッションで生成されたすべてのイベントを復号化してログに記録するかどうかを指定します。メッセージに複数の MIME 添付ファイルが含まれている場合、SMTP インスペクタはファイル名をコンマで区切ってログに記録します。SMTP インスペクタでログに記録できるのは、1024 バイトまでです。

型：ブール値

有効な値：true、false

デフォルト値：false

log_mailfrom

SMTP MAIL FROM コマンドから抽出された送信者の電子メールアドレスとセッションで生成されたすべてのイベントを復号化してログに記録するかどうかを指定します。メッセージに複数の送信者が含まれている場合、SMTP インスペクタは送信者をコンマで区切ってログに記録します。SMTP インスペクタでログに記録できるのは、1024 バイトまでです。

型：ブール値

有効な値：true、false

デフォルト値：false

log_rcptto

SMTP RCPT TO コマンドからの受信者の電子メールアドレスとセッションで生成されたすべてのイベントを復号化してログに記録するかどうかを指定します。メッセージに複数の受信者が含まれている場合、SMTP インスペクタは受信者をコンマで区切ってログに記録します。SMTP インスペクタでログに記録できるのは、1024 バイトまでです。

型：ブール値

有効な値：true、false

デフォルト値：false

max_auth_command_line_len

SMTP 認証コマンドラインで受け入れられる最大バイト数を指定します。

ルール 124:15 を有効にしてイベントを生成し、インライン展開で問題のあるパケットをドロップします。SMTP AUTH コマンドのアラートを無効にするには 0 を指定するか、または Snort 設定の max_auth_command_line_len パラメータを省略します。

型：整数

有効な範囲：0 ～ 65535

デフォルト値：1000

max_command_line_len

SMTP コマンドラインで受け入れられる最大バイト数を指定します。

RFC 2821 の SMTP に関するネットワーク作業部会は、最大コマンドライン長は 512 バイトをお勧めしています。SMTP コマンドライン長でアラートを無効にするには 0 を指定するか、または Snort 設定の `max_command_line_len` パラメータを省略します。

ルール 124:1 を有効にしてイベントを生成し、インライン展開で問題のあるパケットをドロップします。

型：整数

有効な範囲：`0` 〜 `65535`

デフォルト値：`512`

max_header_line_len

SMTP データヘッダー行に許可される最大バイト数を指定します。

RFC 2821 の SMTP に関するネットワーク作業部会は、最大データヘッダー行の長さは 1024 バイトをお勧めしています。SMTP データヘッダー長でアラートを無効にするには 0 を指定するか、または Snort 設定の `max_header_line_len` パラメータを省略します。

ルール 124:2 と 124:7 を有効にしてイベントを生成し、インライン展開で問題のあるパケットをドロップします。

型：整数

有効な範囲：`0` 〜 `65535`

デフォルト値：`1000`

max_response_line_len

SMTP 応答行で受け入れられる最大バイト数を指定します。

RFC 2821 の SMTP に関するネットワーク作業部会は、最大応答行長は 512 バイトをお勧めしています。SMTP 応答行の長さでアラートを無効にするには 0 を指定するか、または Snort 設定の `max_response_line_len` パラメータを省略します。

ルール 124:3 を有効にしてイベントを生成し、インライン展開で問題のあるパケットをドロップします。

型：整数

有効な範囲：`0` 〜 `65535`

デフォルト値：`512`

normalize

すべてのコマンド、コマンドなし、またはコマンドのリストを正規化するかどうかを指定します。コマンドのリストは、`normalize_cmds` パラメータで指定できます。インスペクタは、コマンドの後に複数のスペース（ASCII 0x20）またはタブ（ASCII 0x09）文字を確認します。

型：列挙体

有効な値は、次のとおりです。

- `none`
- `cmds`
- `all`

デフォルト値：`none`

normalize_cmds

正規化する SMTP コマンドのリストを指定します。複数の SMTP コマンドはスペースで区切ります。

型：文字列

有効な値：SMTP コマンド

デフォルト値：なし

qp_decode_depth

各 quoted-printable（QP）エンコード MIME 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。65535 未満の整数を指定するか、または 0 を指定して復号化を無効にすることができます。復号化するバイト数に制限を設定しない場合は、-1 を指定します。

ルール 124:11 を有効にしてイベントを生成し、インライン展開で問題のあるパケットをドロップします。

型：整数

有効な範囲：`-1` 〜 `65535`

デフォルト値：`-1`

uu_decode_depth

各 Unix-to-Unix エンコード（UU エンコード）MIME 電子メール添付ファイルから抽出して復号化できる最大バイト数を指定します。65535 未満の整数を指定するか、または 0 を指定して復号化を無効にすることができます。復号化するバイト数に制限を設定しない場合は、-1 を指定します。

ルール 124:13を有効にしてこのパラメータのイベントを生成し、インライン展開で、（エンコードが正しくないか、またはデータが壊れていることが原因など）復号化が失敗した場合に問題のあるパケットをドロップすることができます。

型：整数

有効な範囲：`-1` 〜 `65535`

デフォルト値：`-1`

valid_cmds

SMTP インスペクタが有効と判断する SMTP コマンドの追加リストを指定します。

SMTP インスペクタは、デフォルトの有効な SMTP コマンド（`ATRN AUTH BDAT DATA DEBUG EHLO EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SIZE STARTTLS SOML TICK TIME TURN TURNME VERB VRFY X-EXPS X-LINK2STATE XADR XAUTH XCIR XEXCH50 XGEN XLICENSE XQUE XSTA XTRN XUSR`）のリストを定義します。

ルール 124:5 を有効にしてイベントを生成し、インライン展開で問題のあるパケットをドロップします。

型：文字列

有効な値：SMTP コマンド

デフォルト値：なし

xlink2state

SMTP インスペクタが X-Link2State Microsoft Exchange バッファ データ オーバーフロー攻撃の一部であるパケットを処理する方法を指定します（脆弱性の説明については、CVE-2005-0560 を参照してください）。検出を無効（`disable`）にし、検出を有効にしてアラートを生成する（`alert`）、または検出を有効にして問題のあるパケットをドロップする（`drop`）ことができます。

このパラメータのイベントを生成し、インライン展開で問題のあるパケットをドロップするには、ルール 124:8 を有効にします。

型：列挙体

有効な値は、次のとおりです。

- `disable`
- `alert`
- `drop`

デフォルト値：`alert`

SMTP インスペクタのルール

`smtp`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 *2 : SMTP* インスペクタのルール

GID:SID	ルール メッセージ
124:1	コマンドバッファのオーバーフローを試行した（attempted command buffer overflow）

GID:SID	ルール メッセージ
124:2	データヘッダーバッファのオーバーフローを試行した（attempted data header buffer overflow）
124:3	応答バッファのオーバーフローを試行した（attempted response buffer overflow）
124:4	特定のコマンドバッファのオーバーフローを試行した（attempted specific command buffer overflow）
124:5	不明なコマンド（unknown command）
124:6	不正なコマンド（illegal command）
124:7	ヘッダー名バッファのオーバーフローを試行した（attempted header name buffer overflow）
124:8	X-Link2State コマンドバッファのオーバーフローを試行した（attempted X-Link2State command buffer overflow）
124:10	Base64 の復号化に失敗した（base64 decoding failed）
124:11	Quoted-Printable の復号化に失敗した（quoted-printable decoding failed）
124:13	Unix-to-Unix の復号化に失敗した（Unix-to-Unix decoding failed）
124:14	Cyrus SASL 認証攻撃（Cyrus SASL authentication attack）
124:15	認証コマンドバッファのオーバーフローを試行した（attempted authentication command buffer overflow）
124:16	ファイルの圧縮解除に失敗した（file decompression failed）

SMTP インスペクタの侵入ルールのオプション

vba_data

検出カーソルを Microsoft Office Visual Basic for Applications マクロバッファに設定します。

シンタックス：`vba_data;`

例：`vba_data;`

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。