SXF 共通ライブラリ　バッファオーバーフローの脆弱性対応について

2015/5/20 OCF事務局

1. 目的

SXF 共通ライブラリにバッファオーバーフローの脆弱性が存在し、改変された sfc ファイルや p21 ファイルを読み込む事と、任意のコードを実行される可能性がありました。この脆弱性に対応すべくライブラリの修正を行いました。

2. 修正の概要

バッファオーバーフローを起こす可能性がある C ランタイムライブラリ（CRT）関数をセキュリティ強化された関数に置き換えました。

SXF 共通ライブラリ Ver.3.21 について修正し、Ver.3.30 としました。

3. 修正内容

SXF 共通ライブラリのプロジェクトに定義されている _CRT_SECURE_NO_WARNINGS を削除してビルドを実行し、警告が出た以下の関数を置き換えました。

strcpy()		strcpy_s()
strncpy()		strncpy_s()
strcat()		strcat_s()
strncat()		strncat_s()
vsprintf()	⇒	vsprintf_s()
_ecvt()		_ecvt_s()
_itoa()		_itoa_s()
fopen()		fopen_s()
strtok()		strtok_s()
sscanf()		sscanf_s()

1) 書き込み先バッファサイズが分かる場合

例）

```
char buf[257];
strcpy(buf,szText);
```

セキュリティ強化された関数に置き換えます。

```
strcpy_s(buf,_countof(buf),szText);
```

2) 書き込み先バッファサイズがその場で分からない場合

例）

```
char buf[257];
func(buf);

void func(char *pOutBuf)
{
    strcpy(pOutBuf,szText);
}
```

関数の引数にサイズを渡すように変更して対応しました。

```
char buf[257];
func(buf,_countof(buf));

void func(char *pOutBuf, size_t BufSize)
{
    strcpy_s(pOutBuf, BufSize ,szText);
}
```

この方針で引数を修正した関数

P21

SXFEntityDataC::SetEntityData()

SXFManageC::Read_next_feature()

SXFMapGeometryC::GetStructData()

SXFPreLineTypeTableC::GetUserLinetype()

SXFReadAP202ManagerC::GetNextFeature()

SXFReadAP202MapManagerC::GetStructData()

SXFutyConvKanjiC::ToJIS()

SXFutyConvKanjiC::FromJIS()

SFC

SXFFeatureC::GetStructData()

SXFManageC::Read_next_feature()

SXFReadFeatureManagerC::GetNextFeature()

SXFReadMapManagerC::GetStructData()

SXFutyConvKanjiC::ConvKanji()

3) 共通ライブラリの外部でバッファが定義されている場合

```
__declspec(dllexport) int WINAPI
        SXFget_file_version_AP202(char OUT_file_version[])
{
    strcpy(OUT_file_version, szVersion);
```

このような公開済み API の引数を変更すると利用者側の修正が必要になってしまうので仕様書に記載されているサイズを固定で使用しました。

```
    strcpy_s(OUT_file_version, 257, szVersion);
```

使用した固定値

SXFopen_part21(), SXFopen_AP202()

ファイル名	file_name	257
ファイル作成者	author	257
作成者所属	organization	257
トランスレータ名	trans_name	257
共通ライブラリバージョン	version	257

SXFread_next_feature(),SXFread_next_feature_AP202()

フィーチャ型	feature_type	64 (注 1)

(注 1) 仕様書には 「型 char *」と書かれていますが実際は利用者側でバッファを確保する必要があります。
ライブラリ内部で使用しているサイズも同梱のサンプルで使用しているサイズも 64 だったのでこれを固定値としました。

SXFget_file_version_part21(),SXFget_file_version_AP202()

SXF ファイルバージョン	file_version	257

4. その他 バグ修正
   - 仕様書の通りに動作していなかった SXFPopMsg(),SXFPopMsg_AP202()を修正しました。
   - 文字列、部分図名称、作図部品名称、作図グループ名称が丁度 256 文字の場合にログファイルにエラーを出力していました。257 文字以上のときにエラーになるように修正しました。(SFC 版を修正、P21 版は問題なし)