Enduro/X Core - Bug #794

ubf user type convert functions might core dump on doubles which representation is larger than 63 symbols

11/10/2022 10:00 PM - Lauris

Status:	Closed	**Start date:**	11/10/2022
Priority:	High (Code 3)	**Due date:**	
Assignee:		**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:			

Description

CB* series of functions as well Bprint might cause core dump, in case if BFLD_FLOAT or BFLD_DOUBLE fields string representation takes more than 63 symbols.
Mainly this affects vast numbers, as places after the comma are limited to 5 (for float) and 6 (for doubles).

Issue is related with temporary space for type conversion which currently is 64 (CF_TEMP_BUF_MAX) and that can make macros like:

```
#define CONV_TO_STRING(X, C) \
    if (CNV_DIR_OUT==cnv_dir && NULL!=out_len)\
    {\
        char tmp[CF_TEMP_BUF_MAX+1];\
        sprintf(tmp, X, (C)*ptr);\
        len = strlen(tmp)+1; /* Including EOS! */\
        if (*out_len<len)\
        {\
            ndrx_Bset_error_fmt(BNOSPACE, "data size: %d specified: %d", len, *out_len);\
            return NULL;\
        }\
        else\
        {\
            strcpy(output_buf, tmp);\
        }\
    }\
    else\
    {\
        /* In case if converting in, we have space for trailing EOS! */\
        sprintf(output_buf, X, (C)*ptr);\
        if (NULL!=out_len) /* In case if we really need it! */\
            len = strlen(output_buf)+1;\
    }\
    if (NULL!=out_len)\
        *out_len = len;\
```

to overflow the buffer.

History

#1 - 11/10/2022 10:03 PM - Lauris

- Description updated

#2 - 11/13/2022 12:45 AM - Lauris

- Priority changed from Normal (Code 4) to High (Code 3)

Release notes

Enduro/X UBF library has been updated, to handle **BFLD_FLOAT** and **BFLD_DOUBLE** fields more safely and accurately in case the value goes beyond 63 digits before the comma (i.e. major unit). This affects CBchg(), Bprint(), Bboolev(), and related functions.

Available from Enduro/X release 7.0.50+, 7.5.38+, 8.0.8+.

#3 - 11/13/2022 12:45 AM - Lauris

- Status changed from New to In Progress

- % Done changed from 0 to 100

#4 - 11/13/2022 12:45 AM - Lauris

- Status changed from In Progress to Closed