Enduro/X Core - Support #505

UBF un-init memory usage

01/16/2020 06:27 PM - Madars

Status: Closed Start date: 01/16/2020

Priority: Normal (Code 4) Due date:

Assignee: % Done: 100%

Category: Estimated time: 0.00 hour

Target version:

Description

==27708== Conditional jump or move depends on uninitialised value(s) ==27708== at 0x55329E6: ubf_cache_update (ubf_impl.c:166)

==27708== by 0x553DCF0: ndrx_Bprojcpy (fproj_impl.c:711)

==27708== by 0x5537763: Bprojcpy (ubf.c:1040) ==27708== by 0x52C6840: OBprojcpy (oubf.c:801)

==27708== by 0x49A342: _cgo_b802f30d0ef5_Cfunc_OBprojcpy (cgo-gcc-prolog:602) ==27708== by 0x457D4F: runtime.asmcgocall (/usr/local/go/src/runtime/asm amd64.s:635)

==27708== by 0xC0000761AF: ???

==27708==

History

#1 - 01/17/2020 03:18 PM - Madars

Seems that this may cause at some rare cases UBF buffer corruption when working with CARRAY fields.

#2 - 01/18/2020 12:24 AM - Madars

 $\underline{https://github.com/endurox-dev/endurox/commit/68 fec1e13739d0bd9aab167db207c9eb00c03501}$

#3 - 01/22/2020 04:58 PM - Madars

- Status changed from New to Resolved
- % Done changed from 0 to 100

Fixed in 7.0.18 +

#4 - 01/22/2020 04:58 PM - Madars

- Status changed from Resolved to Closed

04/19/2024 1/1