

---

Subject: : Odyssey

Topic: : Odyssey 1.23 progress

Re: Odyssey 1.23 progress

Author: : LiveForIt

Date: : 2019/4/6 18:05:43

URL:

@Deniil

Quote:

PPC disassembly:

6fbcec4c: 4bffff84 b 0x6FBCEBD0

6fbcec50: 8124004c lwz r9,76(r4)

\*6fbcec54: 90690000 stw r3,0(r9)

6fbcec58: 4bffff78 b 0x6FBCEBD0

6fbcec5c: 8124004c lwz r9,76(r4)

The debug says it tries to store an int16\_t value from r3 to address of r9.

And r9 was 0x4637C140, not it have been any random value, it possible that memory was corrupted before grim repair detected it. As I have learned it far from built prof.

This thing is not safe at all, not in system with minimum memory protection.