Defect Report

Defect ID: crash_0xffffffff_0x800d800_read_error
Analysis: c50291eb...
Exit Reason: Read to unmapped memory: 0x1079
Total Occurrences: 32,031
Found in Runs: d7244b87
Generated: 3/3/2026, 10:48:50 AM

Classification

Severity: High

Categories: OOBRead, OOBWrite

Root Cause Analysis

Detailed Analysis

The crash occurs due to an out-of-bounds read in HAL_SPI_TxRxCpltCallback. When an SPI transfer completes, the callback reads a 16-bit length value from the beginning of the received SPI data buffer (0x24001800) and uses it as the size parameter for memcpy. The SPI data is read from the peripheral's data register (0x40003c30) one byte at a time during the SPI IRQ handler. The first two bytes received (0x5f and 0x48) form the value 0x485f (18527 bytes), which is used as the copy size without validation.

```
void HAL_SPI_TxRxCpltCallback(SPI_HandleTypeDef *hspi) { // 0x800520c
    ...
    uint16_t len = (uint16_t)0x24001800;  // len = 0x485f (from SPI RX data, unvalidated)
    memcpy(dest_buf, src_buf, len);         // Copies 18527 bytes, far exceeding buffer
    ...
}
```

This massive copy reads beyond the RX buffer and copies MMIO-derived data over adjacent memory structures, including a DMA handle at 0x24006818. The value 0x41a9a1fd overwrites the Parent pointer field at offset 0x38 of the DMA handle (0x24006850). When a DMA error is triggered, SPI_DMAError reads this corrupted pointer and passes it to SPI_CloseTransfer, which dereferences it (loading from address 0x41a9a1fd), then attempts to access offset 0x14 from the loaded value, resulting in an invalid memory access at 0x1079.

Stack Trace

```
0x0800fe26  LoopFillZerobss+0xc
0x080028bc  main+0x2c
0x0800dde4  SPI_DMAError+0x14
```

```
0x0800d800  SPI_CloseTransfer+0x4
```

Proof-of-Concept

Raw Input Data:

```
0x24000800: dd dd
0x40003c00: ea 24 d8 90 e9 49 97 1d 09 89 5b 95 02 02 10 10 04 04 04 04 18 18 18 18 1d 1d 1d 1d 2e
2e
0x40003c04: 2d ee cf 22
0x40003c08: 2e da 3e 6b e2 44 a0 c1 9c bf 1b f4 05 8e 4d 8f 2d 0d 73 95 4c e4 2b 46 00 5b ed 74 0e
69 93 e5 e3 13 93 ce ee 3e 56 ad 04 04 04 04 04 04 04 04 04 04 8a f6 32 a9 73 83 96 d1 34 d5 57 f4
55 b0 32 a9 73 83
0x40003c10: 64 14 cb 1e 10 10 1e da ac ee 63 8f 1c 6d 72 24 c9 d1 0a 0f ac e3 aa 42 aa 42 aa 42
0x40003c14: 2d d7 82 20 18 2c 99 60 09 8c 3b 8e
0x40003c18: fb a1 b3 8e 3c c2 df 5f b7 b1 28 b5 98 e2 ba 72 57 07 26 40 fb a1 98 e2 ba 72 57 80 80
80 80 80 80 80 80 80 80 80 80 80 80 e2 ba 2e 2e 2e 2e 03 03 03 03 20 20 20 20 30 30 30 30 2e 2e
2e 2e 30 30 30 30 2e 2e 2e 2e 34 34 34 34
0x40003c30: 5f 48 76 90 99 ff 19 17 ce 45 c9 7c 90 d0 01 4e 84 16 4a a4 93 50 f6 9d 06 37 e6 0a 85
ec 90 1d 4e ed eb 16 5b 0f 14 2b 4f 40 ca f5 29 1a c6 8c fb 1a 0a cd 19 f6 b2 2f 89 69 52 ec d8 53
44 7c 1c 54 02 58 71 be c3 d3 4f ed 9a 70 9b 00 2c c9 60 c7 43 02 46 18 44 bb f6 ce 63 9b 29 cb 93
0b e3 70 c4 c0 6a c3 cc 1c 7a a7 7e fa ca 25 44 af b3 05 66 f5 09 96 78 5d fd a1 a9 41 6f a6 1e 3b
17 d4 b5 b3 ff 56 71 cb ee 12 bb 77 e4 42 40 dc 69 49 ec b9 2c 18 1d d9 34 0b ae 74 1f 3c fd 8e e6
ea d4 74 d1 08 93 8f 6f 8d fc 4b 15 3e e0 ff 59 a4 76 c7 46 f2 68 bd 05 be 8c 89 2f f3 72 ba ec 53
b0 c7 67 e6 9d 75 c6 5d 84 a8 94 2c 1c 91 67 22 15 7b 3b 1e d5 fa 30 ae 5f 5c 32 bf 7e a9 5b f3 83
c8 2d 56 11 47 ae a1 18 2b f3 79 f3 60 2c 0b ce eb 33 2a 8a b6 de 3d 27 b1 32 9b c4 05
0x40003c50: 67 1c b5 c5
0x40004400: 69 65 a3 79 9e 04 41 6f cc 24 a7 f3 03 1e 6b 12 64 56 86 ab 84 5d ac 99 8d 62 e5 46 ea
f8 df c6 77 1a 88 c1 e1 a7 11 0b a4 92 a4 76 c5 f4
0x40004404: ce e6 cb f9 ca 35 91 e3
0x40004408: ab 43 25 56 ab c1 a4 49 a2 00 cc f9 29 67 5a 6d ad 1e 8d 89 9b bc 6c 89 00 0b 87 96 cd
f4 d8 15 6e be 72 16 3c f0 8c 31
0x4000441c: 04 02 38 3b
0x4000442c: c7 fd a0 3f
0x40020000: 03 7b 3d ab 42 bf 06 b4 ff ff ff ff 70 f6 78 37
0x40020010: d7 d2 84 63 70 a0 a9 d7 eb ce 51 a3 36 88 07 0a 31 4e fb aa 3a c2 52 1b 38 e1 0a 35 70
a0 a9 d7 eb ce 63 70 a0
0x40020024: a3 ec a1 5f 02 02 02 02
0x40020028: 82 5b 71 3c 0a 2e 73 5d 15 d8 f8 4d 98 d7 87 b2 c4 6f 42 1e 15 ab 94 2e 96 b0 d4 70 ff
fb 13 b1
0x4002003c: 75 c8 df ce
0x40020800: e5 a5 e2 00 a4 00 a4
0x40020804: fa 85 00
0x40022008: 97 4a 8a 4c f1 f0 06 1a 9c 49 39 5f 3a 5d f2 b8 d9 2c f2 4c 80 91 ce 6b b0 b8 05 50 7c
18 52 50 d3 21 d1 09 45
0x4002200c: ad 3f fb eb
0x4002201c: 0e 07 84 c1
0x40022030: 2e ef b3 2f 41 90 c3 70
0x400220c0: 34 7e d2 2b
0x40022108: 6a 84 7c eb 29 b0 fd 36 e7 b6 dc a2 2c 6c 4d a0 74 47 a5 48 fe 00 61 30 c1 e5 4b 08 61
cc e5 1c e1 fb 86 fb 6b d3 5d 57 7c
0x4002210c: 4b f6 d6 f0
0x4002211c: a0 c4 7f 07
0x40022130: 81 9d 3d 03 5b 9f fb 7e
0x400221c0: 02 25 cd b1
0x40022308: df 16 e3 77 62 10 e3 d7
0x41a9a1fd: 65
0x41a9a1fe: 10
0x41a9a1ff: 00
0x41a9a200: 00
0x52002000: 4d a6 e5 52
0x5200200c: 9a
0x52002010: 0b 29 cb 09 d4 38 06 e3
0x52002018: 06
0x5200201c: 17 ec ed 79 71 a1
0x52002028: 78 c8 8b 5b
0x52002030: 36 5e 36 0d
0x52002038: e7
0x52002040: 12 fd cf b9
```

```
0x52002048: 61 53 ea 61
0x5200210c: 8a
0x58000000: 57 59 27 74
0x58000004: 25 8f 7c 1f
0x58000080: 8d d7 80 e7
0x58000084: f7 55 55 8d
0x580000e4: e4 c8 d3 04
0x58000414: c1 3b 70 11
0x5800042c: 33 9e 06 03 b5
0x58004008: cb 02 0f e6 09 9a b9 99 f1 a7 f6 3c 01 83 8e 46 ce
0x5800400c: dd cc 11 31 57 e9 4c 4c 6e 61
0x5800404c: c5 29 7a b8 32 ef 5b be
0x5800480c: 00 c3 e1 f4
0x58004810: 36 5c d5 97
0x58020000: fb 21 2a f2 ad aa c3 ea bb 06 4e c2 ca 96 9d 60 7d b7 c0 fb 80 92 e7 d2 ff 13 41 e2 63
6c 7f c3
0x58020004: 5f 0a 8b d3 f8 5b 2c 1c 5e 56 70 1c e7 98 5f 39 38 ff f1 20
0x58020008: f2 4e e0 87 67 9f ba c8 65 31 d0 ec 32 51 c0 35 ab 00 e3 21
0x5802000c: 8a c6 f3 38 bd 56 38 6b 91 21 f2 64 fe 55 e7 1e e3 2c 8b 75 0b cd 27 03 c0 86 c0 f4
0x58020024: 3b 93 a7 82 df 56 d3 88 ff 7f 49 67 87 87 8d 8d 27 ac 1d fd
0x58020400: d2 88 a5 0a
0x58020800: c6 e8 32 b7 95 b0 c8 fa 19 b1 cf 01 8d e2 32 9b 5b b8 1d 52 b5 1b fe 9e 40 80 b2 7f 35
3b cd 0e
0x58020804: 9d 2a 78 66 1a 06 fa 46 f3 4e 63 c3 24 2e f9 ea af 4c 77 8f 7d 68 03 c6 ef c2 b2 bc
0x58020808: 7d d3 4f b6 0c e1 00 68 b5 aa c2 ae f7 e6 69 1b 47 02 4e 88 ea 20 ef 34 35 9f e4 47
0x5802080c: 25 b3 2e d2 d9 0a be 87 09 3f bf 24 6b 68 b9 7b 58 9b 9f a8 16 3b b7 9d 2e 02 f6 25
0x58020810: b8 f8 24 d8 da 62 53 9b 24 d8 da 62 53 d8 da 62
0x58020820: 8f cf 4b af d5 79 92 ca
0x58020824: 92 a0 c4 da 64 a2 87 e4 9d 96 ad a8 25 c5 7e 73
0x58020c00: dc 60 15 98 9f 82 ea 9f cc 08 d0 2a 07 7d 77 ce
0x58020c04: 37 50 b5 dd 26 f2 d4 35 d2 a7 0c 83 4f 31 ac c1
0x58020c08: 24 88 1b a4 a7 21 96 b5 2e 36 f4 da f9 58 1e 7f
0x58020c0c: a0 ad 0d a7 98 88 43 5e 37 00 36 66 bf 0c 8a d7
0x58020c20: 92 1f a7 ea f6 34 dc ec ae 4d 6f ea 9a 2f 26 6d
0x58021400: 75 9a cc 24 97 8a e9 ad 0b 7f 9e ca 88 e7 6f 93 9f 1f ee b3
0x58021800: 67 12 99 92 1f 26 03 0d
0x58021804: 56 77 4a a3 6c 5d 78 90
0x58021808: 79 7b 33 98 0c 6e 6c 48
0x5802180c: 76 ba c2 66 8c 53 4f b9
0x58021820: e6 04 29 af f7 c0 b8 9e
0x58024400: f0 09 52 f7 2f f8 92 49 fe d7 34 5f 0d 6a bb 44 be bd 24 44 82 2c da 99 c5 e2 81 91 14
36 49 82 14 21 0b ff 6f 86 c8 fa 2f 9b e8 dd 82 fe d3 e4 e4 10 1e 27 92 e1 00 cd d1 0e 14 9b 59 bb
7c 92 24 c4 d2 f5 7c af cb 1e 11
0x58024404: fd 79 23 b9
0x58024410: 3e dd 55 47 61 49 c5 6b a9 c8 dc 7a 9e 71 b9 39 15 97 2b 7b de 59
0x58024418: 0d 02 e7 bd c8 b5 69 4a 8d d5 b3 f2 be af 92 c8 a6 25 8f d5 95 ed f8 c0
0x5802441c: 0c 8c 31 d1 0b ec 56 e0 f7 25 ac a9
0x58024420: ad 7c
0x58024428: ca de 36 fc 85 fa 06 b7 13 be 85 87 32 d3 29 5a bc 7e bc 87 00 d1
0x5802442c: 00 df f7 c4 71 fb ea 01 95 4e 42 35 1f 57 d7 a2 91 e0 db 6f ae 63 5b 50 5e 9e bc 30 17
c1 de 49 90 0d 9b 86 04 99 09 86 72 27 27 97 db 58 24 32 94 3d 06 76 b4 e7 65 c7 0f 4c 93 cd ef d4
5a 64 77 7e a6 62 dc 33 d7 a2
0x58024434: e2 e1 16 38
0x5802443c: f0 e9 97 d0 a7 ec 13 aa
0x58024450: eb 59 ee 67 79 2f 47 3e
0x58024454: 9e 63 d5 a1 88
0x58024458: 10 b0 56 54
0x58024470: b3 e8 36 0f f7 75 eb c4 bf 8e f5 1e cf b3 65 ad e1 c1 f8 77 92 84
0x580244d8: fa 1a aa 00 fd 92 ad 25 bf 21 a3 b4 cb 6a d1 82
0x580244dc: 9d 4e 88 58 f8 70 9c 67 07 c7 c6 c5 f1 ea c4 f1 a8 c9
0x580244e0: e2 de fb 73 24 f9 f4 7f f0 b0 58 10 97 34 96 ea 0a 97 ce 93 72 dd 52 92 bb d7 e1 74 d9
fe 72 e2 7c b0 85 d1 9b ee d7 6c 30 c9 e1 c4 00 27 06 e9 dd c8 ec 6b 8e 52 ac bc 3b 84 64 e3 13 eb
94 2d 99 87 3f bf 55 c3 42 ab 41 47 0f 52 54 d6 bd 2f 21 7d b4 7e 79 07 65 cb dc 3d 09 f7 39 90 c5
5e 4c f9 84 e8 8a d9 17 c9 7c 8b 5a 49 c6 b9 c7 9e e9 a3 5b 24 df 4a ed eb 29 2e d3 30 78 7f ab 6e
1a 90 44 92 e7 25 32 4d e0 c9 82 16 0b e3 fa 6e 11 05 51 4a 64 10 e1 c2 96 91 88 7f ef 37 de 18 35
db 1a 2b dc 9d 2c 20 f3 df bf 76 d4 22 34 e9
0x580244e8: c9 18 3a a4 35 0b 08 dc db c7 90 71 a2 f0 3f 19
0x580244f0: 32 ae 30 ce 55 6d 53 5e
0x580244f4: 4c 3f e4 a6 51 70 2d 67 45 55 60 e8 f9
0x58024800: de b9 07 92 69 d9 72 60 7d 68 fd 15 24 cb 59 e6
```

```
0x5802480c: db 24 b4 1b 9b
0x58024818: fb 0c 1c 2d a3 53
0x5802541c: 10 00 09 7f ff ff ff ff 00 00 00 00
0x58026008: 46 16 11 02 29 88 e5 bf 11 db 0e f5 29 07 14 db e8 02 8c 03 a4 ec e6 10 ac 27 26 05 1c
3f 77 34
0x5802600c: 99 e0 68 0a 89 c9
0x58026014: cd f4 e2 c4
0x5802601c: 64 de c1 84
0x58026030: 93 35 5f c0 86 ae 8c 1a
0x58026060: 78
0x58026064: d1
0x58026068: d4
0x5802606c: 76
0x580260c0: f5 03 6b 4a
0x5c001000: f3 8d d2 70 e6 af fd 26 63 2d 60 28 eb 14 cf fb 96 43 bc 40 2f 91 34 9d 63
0xaaaaaaa0: 90 17 30 63 63
```