某局点S6825异常重启问题

软件问题 张文宁 2023-09-29 发表

组网及说明

/

告警信息

/

问题描述

两台堆叠slot2突然异常重启了，需要分析原因：

MPU(S) Slot 2:

Uptime is 0 weeks,0 days,4 hours,6 minutes

H3C S6825-54HF MPU(S) with 1 C3558 Processor(s)

BOARD TYPE: S6825-54HF

DRAM: 4096M bytes

FLASH: 3616M bytes

NVRAM: 0K bytes

PCB 1 Version: VER.A

PCB 2 Version: VER.B

Basic BootWare Version: 136

Extended BootWare Version: 136

CPLD 1 Version: 004

CPLD 2 Version: 002

CPLD 3 Version: 001

Release Version: H3C S6825-54HF-6635

Patch Version: None

Reboot Cause: KernelAbnormalReboot

[SubSlot 0] 48SFP28 + 6QSFP28

过程分析

本次设备重启涉及微码问题，分析过程如下：

1.设备重启前报了invalid opcode无效的操作码，导致设备内核异常重启；

[787121.602685] 3:invalid opcode: 0000 [#1] SMP

[787121.602700] 3:Modules linked in: system(O) addon(O) driver(O)

[787121.602720] 3:CPU: 3 PID: 14134 Comm: bC.0 Tainted: G O 4.4.65 #1

[787121.602738] 3:Hardware name: NONE C3000 Platform1/C3000 Platform1, BIOS 05.10.12.0027 10/26/2018

2.尝试翻译现场异常IP的汇编如下，在正常设备翻译soc_mem_field_get+0x118汇编流程如下，并没有+0x118(+280)的汇编偏移

0x0000000000cbbcde <+270>: add $0x28,%rsp

0x0000000000cbbce2 <+274>: pop %rbx

0x0000000000cbbce3 <+275>: pop %r12

0x0000000000cbbce5 <+277>: pop %r13

0x0000000000cbbce7 <+279>: pop %r14

0x0000000000cbbce9 <+281>: pop %r15//并没有偏移+280的汇编指令

0x0000000000cbbceb <+283>: pop %rbp

0x0000000000cbbcec <+284>: retq

0x0000000000cbbced <+285>: nopl (%rax)

0x0000000000cbbcf0 <+288>: mov 0x0(,%r12,8),%rax

0x0000000000cbbcf8 <+296>: mov $0x0,%r8

3.现场dump出的代码段信息与正常设备的代码段一致，不存在差异，排除代码段导致的异常；

[787121.630417] 3:Code: 94 03 48 8b 40 48 4a 8b 34 e0 48 8b 55 c8 41 b9 14 00 00 00 4d 89 f8 44 89 f1 89 df e8 c2 e6 ff ff 48 83 c4 28 5b 41 5c 41 5d 41 <5e> 41 5f 5d c3 0f 1f 00 4a 8b 04 e5 a0 05 b3 a4 49 c7 c0 00 c8

正常设备的代码段：

(gdb) x/32xb 0x0000000000cbbce2

0xcbbce2 <soc_mem_field_get+274>: 0x5b 0x41 0x5c 0x41 0x5d 0x41 0x5e 0x41

0xcbbcea <soc_mem_field_get+282>: 0x5f 0x5d 0xc3 0x0f 0x1f 0x00 0x4a 0x8b

0xcbbcf2 <soc_mem_field_get+290>: 0x04 0xe5 0x00 0x00 0x00 0x00 0x49 0xc7

0xcbbcfa <soc_mem_field_get+298>: 0xc0 0x00 0x00 0x00 0x00 0x45 0x89 0xd9

综合来看，触发异常的原因是CPU执行汇编指令运行结果不符合预期，导致设备触发异常，涉及C3000 CPU微码指令执行出错的问题，建议安装最新的强补丁解决，合入了最新的微码版本；

解决方法

综合来看，触发异常的原因是CPU执行汇编指令运行结果不符合预期，导致设备触发异常，涉及C3000 CPU微码指令执行出错的问题，建议安装最新的强补丁解决，合入了最新的微码版本；