


```
V2 : 00FF00FF00FF00FF17E817E88A758A75 00000000000000000000000000000000
V4 : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF 01FF01FF01FF01FF09F709F7DB25DB25
V6 : 7A8500FF0DF200FF18E708F7EC13DA25 00000000010101010202020203030303
V8 : 00FF00FF00FF00FF08F708F7DA25DA25 01FF01FF01FF01FF18E818E88B758B75
V10: 0101010101010101181818188B8B8B8B 00000000000000000000000000000000
V12: 00FF00FF00FF00FF17E817E88A758A75 FFF08080FFF08080FFF08080FFF08080
V14: 001002120414061608180A1A0C1C0E1E 01000100010001000100010001000100
V16: FF000000FF000000FF000000FF000000 0101010101010101181818188B8B8B8B
V18: 00000000000000000000000000000000 01FF01FF01FF01FF18E818E88B758B75
V20: 00000000000000000000000000000000 00000000000000000000000000000000
V22: 00000000000000000000000000000000 00000000000000000000000000000000
V24: 00000000000000000000000000000000 00000000000000000000000000000000
V26: 00000000000000000000000000000000 00000000000000000000000000000000
V28: 00000000000000000000000000000000 00000000000000000000000000000000
V30: 00000000000000000000000000000000 00000000000000000000000000000000
VSCR: 00000000 VRSAVE: 00000000
```

Disassembly of crash site:

```
020395C0: 7FA4EB78 mr r4,r29
020395C4: 7D2903A6 mtctr r9
020395C8: 4E800421 bctrl
020395CC: 815E0020 lwz r10,32(r30)
>020395D0: 813D005C lwz r9,92(r29)
020395D4: 7D295050 sub r9,r10,r9
020395D8: 913E0020 stw r9,32(r30)
020395DC: 80010024 lwz r0,36(r1)
020395E0: 8361000C lwz r27,12(r1)
020395E4: 7C0803A6 mtlr r0
```

Kernel command line: serial munge debuglevel=1

Registers pointing to code:

```
r0 : native kernel module kernel+0x000394fc
r3 : native kernel module kernel+0x00973054
r6 : native kernel module dos.library.kmod+0x0002f1fc
r8 : native kernel module kernel+0x00a8f000
r9 : native kernel module kernel+0x00031028
r11: native kernel module kernel+0x0001ed14
r14: native kernel module dos.library.kmod+0x000159f8
r15: native kernel module kernel+0x00973054
r17: native kernel module graphics.library.kmod+0x00860580
r18: native kernel module kernel+0x0002bde4
r22: native kernel module dos.library.kmod+0x00702258
r23: native kernel module graphics.library.kmod+0x00860580
r30: native kernel module kernel+0x00a956f0
r31: native kernel module kernel+0x00973054
ip : native kernel module kernel+0x000395d0
lr : native kernel module kernel+0x000395cc
ctr: native kernel module kernel+0x00031028
```

Stack trace:

V26: 00000000000000000000000000000000 00000000000000000000000000000000
V28: 00000000000000000000000000000000 00000000000000000000000000000000
V30: 00000000000000000000000000000000 00000000000000000000000000000000
VSCR: 00000000 VRSAVE: 00000000

Disassembly of crash site:

7FDD4BD4: 4BFFFDC8 b 0x7FDD499C
7FDD4BD8: A0030020 lhz r0,32(r3)
7FDD4BDC: 7FE02214 add r31,r0,r4
7FDD4BE0: 83BF0010 lwz r29,16(r31)
>7FDD4BE4: 839D0000 lwz r28,0(r29)
7FDD4BE8: 2F9C0000 cmpwi cr7,r28,0
7FDD4BEC: 40BE005C bne+ cr7,0x7FDD4C48
7FDD4BF0: 480000D8 b 0x7FDD4CC8
7FDD4BF4: A81D0018 lha r0,24(r29)
7FDD4BF8: 2F800000 cmpwi cr7,r0,0
(0x61A7F370) module AmiDock at 0x7F981108 (section 5 @ 0x270E4)
(0x61A7F380) module AmiDock at 0x7F979084 (section 5 @ 0x1F060)
(0x61A7F550) module AmiDock at 0x7F95F870 (section 5 @ 0x584C)
(0x61A7F9E0) module AmiDock at 0x7F95BB08 (section 5 @ 0x1AE4)
(0x61A7FA80) module AmiDock at 0x7F95C330 (section 5 @ 0x230C)
(0x61A7FCE0) module AmiDock at 0x7F95C404 (section 5 @ 0x23E0)
(0x61A7FD00) native kernel module newlib.library.kmod+0x000020a4
(0x61A7FD70) native kernel module newlib.library.kmod+0x00002d54
(0x61A7FF10) native kernel module newlib.library.kmod+0x00002ee8
(0x61A7FF50) module AmiDock at 0x7F95A190 (section 5 @ 0x16C)
(0x61A7FF90) native kernel module dos.library.kmod+0x000255c8
(0x61A7FFC0) native kernel module kernel+0x000420ac
(0x61A7FFD0) native kernel module kernel+0x000420f4

Disassembly of crash site:

020395C0: 7FA4EB78 mr r4,r29
020395C4: 7D2903A6 mtctr r9
020395C8: 4E800421 bctrl
020395CC: 815E0020 lwz r10,32(r30)
>020395D0: 813D005C lwz r9,92(r29)
020395D4: 7D295050 sub r9,r10,r9
020395D8: 913E0020 stw r9,32(r30)
020395DC: 80010024 lwz r0,36(r1)
020395E0: 8361000C lwz r27,12(r1)
020395E4: 7C0803A6 mtlr r0

Stack pointer (0x61A7EFD0) is inside bounds

Redzone is OK (4)

68k register dump

DATA: 00000001 00000000 00000000 00000000 00000000 00000000 00000000 00000000
----> 00000001 - "CLASSES:datatypes/logfile.datatype" Hunk 0000 Offset 00000000 (SegList: 0x13826845)
ADDR: 6FFB8700 96213400 00000000 00000000 00000000 00000000 00000000 61A7EEE0

Page information:

Page not found

[DOS] ERROR in System(), CloneTagItems() failed.

GrimReaper launch failed

Kernel command line: serial munge debuglevel=1

Registers pointing to code:

r11: native kernel module graphics.library.kmod+0x00860580

rip : module CLASSES:gadgets/layout.gadget at 0x7FDD4BE4 (section 5 @ 0x8BC0)

lr : native kernel module intuition.library.kmod+0x00021448

ctr: module CLASSES:gadgets/layout.gadget at 0x7FDD47A4 (section 5 @ 0x8780)

Stack trace:

(0x4EECA100) module CLASSES:gadgets/layout.gadget at 0x7FDD4BE4 (section 5 @ 0x8BC0)

(0x4EECA2A0) native kernel module intuition.library.kmod+0x00021448

(0x4EECA300) native kernel module intuition.library.kmod+0x000215ec

(0x4EECA380) native kernel module intuition.library.kmod+0x0000a2d8

(0x4EECA390) native kernel module intuition.library.kmod+0x00009f8c

(0x4EECA400) module CLASSES:gadgets/layout.gadget at 0x7FDD4730 (section 5 @ 0x870C)

(0x4EECA450) module CLASSES:gadgets/layout.gadget at 0x7FDD4E8C (section 5 @ 0x8E68)

(0x4EECA5F0) native kernel module intuition.library.kmod+0x00021448

(0x4EECA650) native kernel module intuition.library.kmod+0x000215ec

(0x4EECA6D0) native kernel module intuition.library.kmod+0x0000a348

(0x4EECA700) native kernel module intuition.library.kmod+0x0000a0dc

(0x4EECA770) module CLASSES:requester.class at 0x7F8FDD10 (section 5 @ 0x2CEC)

(0x4EECAAB0) native kernel module intuition.library.kmod+0x00021448

(0x4EECAB10) native kernel module intuition.library.kmod+0x000215ec

(0x4EECAB90) native kernel module intuition.library.kmod+0x0000a3f4

(0x4EECABA0) module IPrefs at 0x7FF353F4 (section 5 @ 0xF3D0)

(0x4EECAC00) native kernel module dos.library.kmod+0x0003388c

(0x4EECAD40) native kernel module dos.library.kmod+0x00026580

(0x4EECB080) native kernel module dos.library.kmod+0x0000df18

(0x4EECB0A0) native kernel module dos.library.kmod+0x0000e328

(0x4EECB300) native kernel module dos.library.kmod+0x00023a60

(0x4EECB370) module SYS:System/AmiUpdate/AmiUpdate at 0x7F66284C (section 5 @ 0x21828)

(0x4EECB470) module SYS:System/AmiUpdate/AmiUpdate at 0x7F663574 (section 5 @ 0x22550)

(0x4EECDE20) module SYS:System/AmiUpdate/AmiUpdate at 0x7F6486D4 (section 5 @ 0x76B0)

(0x4EED4330) module SYS:System/AmiUpdate/AmiUpdate at 0x7F64ACA0 (section 5 @ 0x9C7C)

(0x4EED4380) module SYS:System/AmiUpdate/AmiUpdate at 0x7F64C6C0 (section 5 @ 0xB69C)

(0x4EED4450) module SYS:System/AmiUpdate/AmiUpdate at 0x7F64F494 (section 5 @ 0xE470)

(0x4EED4CF0) native kernel module newlib.library.kmod+0x000020a4

(0x4EED4D60) native kernel module newlib.library.kmod+0x00002d0c

(0x4EED4F00) native kernel module newlib.library.kmod+0x00002ee8

(0x4EED4F40) module SYS:System/AmiUpdate/AmiUpdate at 0x7F641194 (section 5 @ 0x170)

(0x4EED4F90) native kernel module dos.library.kmod+0x000255c8

(0x4EED4FC0) native kernel module kernel+0x000420ac

(0x4EED4FD0) native kernel module kernel+0x000420f4

Disassembly of crash site:

7FDD4BD4: 4BFFFDC8 b

0x7FDD499C

```
7FDD4BD8: A0030020 lhz      r0,32(r3)
7FDD4BDC: 7FE02214  add      r31,r0,r4
7FDD4BE0: 83BF0010  lwz      r29,16(r31)
>7FDD4BE4: 839D0000  lwz      r28,0(r29)
7FDD4BE8: 2F9C0000  cmpwi    cr7,r28,0
7FDD4BEC: 40BE005C  bne+     cr7,0x7FDD4C48
7FDD4BF0: 480000D8  b        0x7FDD4CC8
7FDD4BF4: A81D0018  lha      r0,24(r29)
7FDD4BF8: 2F800000  cmpwi    cr7,r0,0
```

Stack pointer (0x4EECA100) is inside bounds

Redzone is OK (4)

68k register dump

```
DATA: 00000001 00000000 00000000 00000000 00000000 00000000 00000000 00000000
----> 00000001 - "CLASSES:datatypes/logfile.datatype" Hunk 0000 Offset 00000000 (SegList: 0x13826845)
ADDR: 6FFB8700 96189900 00000000 00000000 00000000 00000000 00000000 4EED3660
```

Page information:

Page not found

[DOS] ERROR in System(), CloneTagItems() failed.

GrimReaper launch failed

Just copy the two files below anywhere and start the guide, click on crash and, well, crash

crash.guide

```
@DATABASE Crash
@NODE "main" "crash"
@{"Crash!" LINK crash.txt/main}
@ENDNODE
```

crash.txt

```
l: [15:47:34]          USB stack |           | =====
l: [15:47:34]          USB stack |           | USB System Software Task started
l: [15:47:34]          USB stack |           | Starting HCDs...
l: [15:47:34]          USB stack |           | New Fkt | Fkt 0x6FF8FBE0 at level -1
l: [15:47:34]          USB stack |           | New Fkt | Fkt 0x6FF8FC80 at level 0
l: [15:47:35]          USB stack |           | New Fkt | Fkt 0x6FF8FD20 at level -1
l: [15:47:35]          USB stack |           | New Fkt | Fkt 0x6FF8FDC0 at level 0
l: [15:47:35]          USB stack |           | New Fkt | Fkt 0x6FF8FE60 at level -1
l: [15:47:35]          USB stack |           | New Fkt | Fkt 0x6FF8FF00 at level 0
l: [15:47:35]          USB stack |           | New Fkt | Fkt 0x6FD3A010 at level -1
l: [15:47:35]          USB stack |           | New Fkt | Fkt 0x6FD3A0B0 at level 0
l: [15:47:36]          USB stack |           | New Fkt | Fkt 0x6FD3A150 at level -1
l: [15:47:36]          USB stack |           | New Fkt | Fkt 0x6FD3A1F0 at level 0
l: [15:47:36]          USB stack |           | New Fkt | Fkt 0x6FD3A290 at level -1
l: [15:47:36]          USB stack |           | New Fkt | Fkt 0x6FD3A330 at level 0
```



```
[15:47:36] USB stack | ...HCDs started.
l: [15:47:36] USB Fkt Init | Init Fkt | Fkt 0x6FF8FC80 is {Vendor: 0x0000, Product:
0x0000, Class: 09.00}
l: [15:47:36] USB Fkt Init | Init Fkt | Fkt 0x6FF8FDC0 is {Vendor: 0x0000, Product:
0x0000, Class: 09.00}
l: [15:47:36] USB Fkt Init | Init Fkt | Fkt 0x6FF8FF00 is {Vendor: 0x0000, Product:
0x0000, Class: 09.00}
l: [15:47:36] USB Fkt Init | Init Fkt | Fkt 0x6FD3A0B0 is {Vendor: 0x0000, Product:
0x0000, Class: 09.00}
l: [15:47:36] USB Fkt Init | Init Fkt | Fkt 0x6FD3A1F0 is {Vendor: 0x0000, Product:
0x0000, Class: 09.00}
l: [15:47:36] USB Fkt Init | Init Fkt | Fkt 0x6FD3A330 is {Vendor: 0x0000, Product:
0x0000, Class: 09.00}
l: [15:47:36] USB Fkt Init | Init Fkt | Fkt 0x6FF8FC80 initialized
l: [15:47:36] USB Fkt Init | Init Fkt | Fkt 0x6FF8FDC0 initialized
l: [15:47:36] USB Fkt Init | Init Fkt | Fkt 0x6FF8FF00 initialized
l: [15:47:36] USB Fkt Init | Init Fkt | Fkt 0x6FD3A0B0 initialized
l: [15:47:36] USB Fkt Init | Init Fkt | Fkt 0x6FD3A1F0 initialized
l: [15:47:36] USB Fkt Init | Init Fkt | Fkt 0x6FD3A330 initialized
l: [15:47:36] hub.usbfd | HUB | Hub "Rear Roothub (ohci.usbhcd/0)"
has TT thinktime of 8 full speed bittimes and protocol 0
l: [15:47:36] hub.usbfd | HUB | Hub "Front Roothub (ohci.usbhcd/1)"
has TT thinktime of 8 full speed bittimes and protocol 0
l: [15:47:36] hub.usbfd | HUB | Hub "Additional Roothub (ohci.usbhcd)"
has TT thinktime of 8 full speed bittimes and protocol 0
l: [15:47:36] hub.usbfd | HUB | Hub "Additional Roothub (ohci.usbhcd)"
has TT thinktime of 8 full speed bittimes and protocol 0
l: [15:47:36] hub.usbfd | HUB | All ports are empty
l: [15:47:36] hub.usbfd | HUB | All ports are empty
l: [15:47:36] hub.usbfd | HUB | Hub "Additional Roothub (ohci.usbhcd)"
has TT thinktime of 8 full speed bittimes and protocol 0
l: [15:47:36] hub.usbfd | HUB | All ports are empty
l: [15:47:36] hub.usbfd | HUB | Hub "Rear Roothub (ehci.usbhcd/0)"
has TT thinktime of 8 full speed bittimes and protocol 0
l: [15:47:36] hub.usbfd | HUB | All ports are empty
l: [15:47:36] hub.usbfd | HUB | All ports are empty
l: [15:47:36] EHCI Controller Task Unit 0 | EHCI | Device at port 6 is a lowspeed device.
Giving up ownership.
l: [15:47:36] EHCI Controller Task Unit 0 | EHCI | Device at port 7 is a lowspeed device.
Giving up ownership.
l: [15:47:36] hub.usbfd | HUB | Device found on port 2 of hub
"Rear Roothub (ehci.usbhcd/0)".
l: [15:47:36] hub.usbfd | HUB | Device found on port 1 of hub
"Additional Roothub (ohci.usbhcd)".
l: [15:47:36] EHCI Controller Task Unit 0 | EHCI | Device at port 1 is a fullspeed device.
Giving up ownership.
l: [15:47:36] hub.usbfd | HUB | Port 2 of hub "Rear Roothub (ehci.usbhcd/0)"
reset timed out
W: [15:47:36] hub.usbfd | HUB | Resetting hub port 2 and trying again
l: [15:47:36] hub.usbfd | Hub port | Device at port 1 of hub
"Additional Roothub (ohci.usbhcd)" is low-speed.
```

```
[15:47:36] hub.usbfd | HUB | Reset request for port 2 failed (error -23)
E: [15:47:36] hub.usbfd | HUB | Resetting port 2 of hub
"Rear Roothub (ehci.usbhcd/0)" failed. Device adding aborted
I: [15:47:36] hub.usbfd | HUB | Device found on port 9 of hub
"Rear Roothub (ehci.usbhcd/0)".
I: [15:47:36] USB stack | New Fkt | Fkt 0x6FD3A790 at level 1
I: [15:47:36] hub.usbfd | HUB | Device on hub port 1 successfully added.
I: [15:47:36] hub.usbfd | HUB | Device found on port 2 of hub
"Additional Roothub (ohci.usbhcd)".
I: [15:47:36] USB Fkt Init | Init Fkt | Fkt 0x6FD3A790 is {Vendor: 0x04F2, Product:
0x0116, Class: 00.00}
I: [15:47:36] USB Fkt Init | Init Fkt | Fkt 0x6FD3A790 initialized
I: [15:47:37] hub.usbfd | Hub port | Device at port 2 of hub
"Additional Roothub (ohci.usbhcd" is low-speed.
I: [15:47:37] USB stack | New Fkt | Fkt 0x6FD3A830 at level 1
I: [15:47:37] hub.usbfd | HUB | Device on hub port 2 successfully added.
I: [15:47:37] USB Fkt Init | Init Fkt | Fkt 0x6FD3A830 is {Vendor: 0x1BCF, Product:
0x0005, Class: 00.00}
I: [15:47:37] USB Fkt Init | Init Fkt | Fkt 0x6FD3A830 initialized
I: [15:47:37] hub.usbfd | Hub port | Device at port 9 of hub
"Rear Roothub (ehci.usbhcd/0)" is high-speed.
I: [15:47:37] USB stack | New Fkt | Fkt 0x6FD3A8D0 at level 1
I: [15:47:37] hub.usbfd | HUB | Device on hub port 9 successfully added.
I: [15:47:37] EHCI Controller Task Unit 0 | EHCI | Port 8 is not in reset state.
I: [15:47:37] hub.usbfd | HUB | Device found on port 10 of hub
"Rear Roothub (ehci.usbhcd/0)".
I: [15:47:37] USB Fkt Init | Init Fkt | Fkt 0x6FD3A8D0 is {Vendor: 0x05E3, Product:
0x0608, Class: 09.00}
I: [15:47:37] USB Fkt Init | Init Fkt | Fkt 0x6FD3A8D0 initialized
I: [15:47:37] hub.usbfd | HUB | Hub "USB2.0 Hub"
has TT thinktime of 32 full speed bittimes and protocol 1
I: [15:47:37] hub.usbfd | HUB | Device found on port 2 of hub
"Rear Roothub (ohci.usbhcd/0)".
I: [15:47:37] hub.usbfd | Hub port | Device at port 10 of hub
"Rear Roothub (ehci.usbhcd/0)" is high-speed.
I: [15:47:37] hub.usbfd | Hub port | Device at port 2 of hub
"Rear Roothub (ohci.usbhcd/0)" is full-speed.
I: [15:47:37] USB stack | New Fkt | Fkt 0x6FD3AA10 at level 1
I: [15:47:37] hub.usbfd | HUB | Device on hub port 10 successfully added.
I: [15:47:37] EHCI Controller Task Unit 0 | EHCI | Port 9 is not in reset state.
I: [15:47:37] hub.usbfd | HUB | Driver Running
I: [15:47:37] USB Fkt Init | Init Fkt | Fkt 0x6FD3AA10 is {Vendor: 0x05E3, Product:
0x0608, Class: 09.00}
I: [15:47:37] USB Fkt Init | Init Fkt | Fkt 0x6FD3AA10 initialized
I: [15:47:37] USB stack | New Fkt | Fkt 0x6FD3AAB0 at level 1
I: [15:47:37] hub.usbfd | HUB | Device on hub port 2 successfully added.
I: [15:47:37] hub.usbfd | HUB | Hub "USB2.0 Hub"
has TT thinktime of 32 full speed bittimes and protocol 1
I: [15:47:37] USB Fkt Init | Init Fkt | Fkt 0x6FD3AAB0 is {Vendor: 0x0582, Product:
0x0052, Class: 00.00}
I: [15:47:37] USB Fkt Init | Init Fkt | Fkt 0x6FD3AAB0 initialized
```


