pfSense - Bug #4689

Panic/Crash "sbflush_internal: cc 4294967166 || mb 0 || mbcnt 0"

05/08/2015 12:28 PM - Jim Pingle

Status:	Resolved	**Start date:**	05/08/2015
Priority:	Normal	**Due date:**	
Assignee:	Jim Pingle	**% Done:**	0%
Category:	Operating System	**Estimated time:**	0.00 hour
Target version:	2.4.0		
Affected Version:	2.3	**Affected Architecture:**	All

Description

Exact cause yet unknown, but a panic can be triggered with the above condition. It appears to be a FreeBSD bug with a known fix which can be backported.

Crash report details:

```
Dump header from device /dev/da0s1b
  Architecture: amd64
  Architecture Version: 1
  Dump Length: 157184B (0 MB)
  Blocksize: 512
  Dumptime: Fri May  8 00:00:22 2015
  Magic: FreeBSD Text Dump
  Version String: FreeBSD 10.1-RELEASE-p6 #0 b69ba8f(releng/10.1)-dirty: Fri Mar 13 08:37:46 CDT 2
015
    root@pfs22-amd64-builder:/usr/obj.amd64/usr/pfSensesrc/src/sys/pfSense_SMP.10
  Panic String: sbflush_internal: cc 4294967166 || mb 0 || mbcnt 0
  Dump Parity: 2721008901
  Bounds: 0
  Dump Status: good
```

```
db:0:kdb.enter.default>  show pcpu
cpuid        = 0
dynamic pcpu = 0x638780
curthread    = 0xffffff80037e02490: pid 71027 "miniupnpd"
curpcb       = 0xffffffe000030ab80
fpcurthread  = 0xffffff80037e02490: pid 71027 "miniupnpd"
idlethread   = 0xffffff80003292000: tid 100003 "idle: cpu0"
curpmap      = 0xffffff80100093d78
tssp         = 0xffffffff82194f90
commontssp   = 0xffffffff82194f90
rsp0         = 0xffffffe000030ab80
gs32p        = 0xffffffff821969e8
ldt          = 0xffffffff82196a28
tss          = 0xffffffff82196a18
db:0:kdb.enter.default>  bt
Tracing pid 71027 tid 100151 td 0xffffff80037e02490
kdb_enter() at kdb_enter+0x3e/frame 0xffffffe000030a740
panic() at panic+0x175/frame 0xffffffe000030a7c0
sbflush_internal() at sbflush_internal+0x7b/frame 0xffffffe000030a7e0
sbflush() at sbflush+0x46/frame 0xffffffe000030a810
tcp_disconnect() at tcp_disconnect+0x52/frame 0xffffffe000030a840
tcp_usr_disconnect() at tcp_usr_disconnect+0x84/frame 0xffffffe000030a870
soclose() at soclose+0x3c/frame 0xffffffe000030a8b0
_fdrop() at _fdrop+0x29/frame 0xffffffe000030a8d0
closef() at closef+0x21e/frame 0xffffffe000030a960
```

```
closefp() at closefp+0x98/frame 0xfffffe000030a9a0
amd64_syscall() at amd64_syscall+0x351/frame 0xfffffe000030aab0
Xfast_syscall() at Xfast_syscall+0xfb/frame 0xfffffe000030aab0
```

Tail end of the message buffer:

```
<7>sonewconn: pcb 0xfffff800224167a8: Listen queue overflow: 8 already in queue awaiting acceptanc
e (4 occurrences)
<7>sonewconn: pcb 0xfffff800224167a8: Listen queue overflow: 8 already in queue awaiting acceptanc
e (13 occurrences)
<7>sonewconn: pcb 0xfffff800224167a8: Listen queue overflow: 8 already in queue awaiting acceptanc
e (8 occurrences)
vmx0: watchdog timeout on queue 0
vmx0: watchdog timeout on queue 0
vmx0: watchdog timeout on queue 0
vmx0: watchdog timeout on queue 0
vmx0: watchdog timeout on queue 0
vmx0: watchdog timeout on queue 0
vmx0: watchdog timeout on queue 0
vmx0: watchdog timeout on queue 0
vmx0: watchdog timeout on queue 0
vmx0: watchdog timeout on queue 0
vmx0: watchdog timeout on queue 0
vmx0: watchdog timeout on queue 0
vmx0: watchdog timeout on queue 0
vmx0: watchdog timeout on queue 0
vmx0: watchdog timeout on queue 0
panic: sbflush_internal: cc 4294967166 || mb 0 || mbcnt 0
cpuid = 0
KDB: enter: panic
```

See also: OCK-41128

History

#1 - 05/13/2015 03:27 PM - Ermal Luçi

- Status changed from New to Feedback

Merged patch.

#2 - 06/21/2015 04:06 PM - Chris Buechler

- Target version changed from 2.2.3 to 2.3

- Affected Version changed from 2.2.2 to 2.2.x

no known way to replicate this. Likely fixed with the patch that's been merged but will leave for feedback.

#3 - 08/31/2015 09:26 PM - Jim Thompson

- Assignee changed from Ermal Luçi to Chris Buechler

reassign

#4 - 11/18/2015 05:39 PM - Chris Buechler

- Status changed from Feedback to Resolved

fixed in FreeBSD

#5 - 11/17/2016 06:07 PM - Claude Duvergier

I am getting this symptom (crashs) on v2.3.2, multiple times a day:

```
Crash report begins.  Anonymous machine information:

amd64
10.3-RELEASE-p9
FreeBSD 10.3-RELEASE-p9 #1 5fc1b19(RELENG_2_3_2): Tue Sep 27 12:26:06 CDT 2016     root@ce23-amd64-builder:/bu
ilder/pfsense-232/tmp/obj/builder/pfsense-232/tmp/FreeBSD-src/sys/pfSense

Crash report details:

Filename: /var/crash/bounds
1

Filename: /var/crash/info.0
Dump header from device /dev/label/swap0
  Architecture: amd64
  Architecture Version: 1
  Dump Length: 80896B (0 MB)
  Blocksize: 512
  Dumptime: Wed Nov  2 13:21:44 2016
  Hostname: hermes.example.com
  Magic: FreeBSD Text Dump
  Version String: FreeBSD 10.3-RELEASE-p9 #1 5fc1b19(RELENG_2_3_2): Tue Sep 27 12:26:06 CDT 2016
    root@ce23-amd64-builder:/builder/pfsense-232/tmp/obj/builder/pfsense-232/tmp/FreeBSD-src/sys/pfSense
  Panic String: sbflush_internal: cc 4294965256 || mb 0 || mbcnt 0
  Dump Parity: 916287357
  Bounds: 0
  Dump Status: good
```

(see forum and full report)

Also, someone on FreeBSD bugtracker reported the bug is still there on a 10-STABLE a month ago.

#6 - 12/14/2016 07:15 AM - Jim Pingle

- Status changed from Resolved to New

- Assignee changed from Chris Buechler to Jim Thompson

- Target version changed from 2.3 to 2.4.0

- Affected Version changed from 2.2.x to 2.3

This is still happening to customers on 2.3.2-p1, so the imported patch didn't fix the problem.

#7 - 09/11/2017 12:10 AM - Jim Thompson

- Assignee changed from Jim Thompson to Jim Pingle

does anyone see this on 2.3 (and an 11.0 base)?

#8 - 09/11/2017 08:14 AM - Jim Pingle

- Status changed from New to Resolved

The FreeBSD bug report is still open, though it doesn't contain any reports of issues on 11.x. I haven't seen any recent reports of this issue either. There were some claims it was happening on 2.4 late last year but searching around I don't see anything current. The reports someone posted for 2.4 also don't match this panic message exactly.

The reports for the similar crash on 2.4, "panic: sbsndptr: sockbuf <x> and mbuf <y> clashing" (https://bugs.freebsd.org/bugzilla/show_bug.cgi?id=213257 and https://bugs.freebsd.org/bugzilla/show_bug.cgi?id=212413) have been patched and I don't see anything recent from them either.

Looks like we can close this out for now. If there are more reports we can kick this forward to 2.4.1 and see how 11.1 behaves.