pYIN — pitch and note tracking in monophonic audio - Bug #914
Buffer overrun in YinUtil::yinProb

2014-04-01 11:01 AM - Chris Cannam

Status:	Resolved	**Start date:**	2014-04-01
Priority:	Normal	**Due date:**	
Assignee:	Matthias Mauch	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			

Description

spotted while running Valgrind on Tony:
3564 Invalid read of size 8
3564 at 0x626A25D: YinUtil::yinProb(double const*, unsigned long, unsigned long, unsigned long, unsigned long) (YinUtil.cpp:278)
3564 by 0x6267EC7: Yin::processProbabilisticYin(double const*) const (Yin.cpp:92)
3564 by 0x624432F: PYinVamp::process(float const* const*, _VampPlugin::Vamp::RealTime) (PYinVamp.cpp:372)
...
3564 Address 0xc2ac340 is 0 bytes after a block of size 8,192 alloc'd
3564 at 0x4C293B0: operator new[](unsigned long) (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
3564 by 0x6267E62: Yin::processProbabilisticYin(double const*) const (Yin.cpp:86)
3564 by 0x624432F: PYinVamp::process(float const* const*, _VampPlugin::Vamp::RealTime) (PYinVamp.cpp:372)
Looks like tau == maxTau-1 and so yinBuffer[tau+1] is yinBuffer[yinBufferSize] which (being zero-based) is indexing just beyond the end of the array.

History

#1 - 2014-04-01 11:06 AM - Chris Cannam

- Status changed from New to Resolved

- Assignee set to Matthias Mauch

Likely fix committed in commit:da92a0abc7c6 (for review)

#2 - 2014-04-01 12:45 PM - Matthias Mauch

Thanks, that was quick. Just wanted to look into it. M