PL/php - Bug #4975

RETURNS RECORD can crash the server

11/30/2005 05:53 AM - Álvaro Herrera

Status:	Closed	**Start date:**	
Priority:	Immediate	**Due date:**	
Assignee:	Álvaro Herrera	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	Release 1.1		
Resolution:	fixed		

Description

A trivial "RETURNS RECORD" function can crash the server. An example:

```
CREATE OR REPLACE FUNCTION php_record(integer) RETURNS record
LANGUAGE plphp AS $$
        $ret['f1']=$argsr0;
        $ret['f2']="hello";
        $ret['f3']="world";
        return $ret;
$$;
```

Calling this function as

```
SELECT * FROM php_record(1) AS (f1 integer, f2 text, f3 text);
```

crashes the server and leaves a coredump with the following backtrace:

```
#0  pg_detoast_datum (datum=0x7f7f7f7f)
    at /pg/source/00orig/src/backend/utils/fmgr/fmgr.c:1798
1798            if (VARATT_IS_EXTENDED(datum))
(gdb) bt
#0  pg_detoast_datum (datum=0x7f7f7f7f)
    at /pg/source/00orig/src/backend/utils/fmgr/fmgr.c:1798
#4964  0x08145f6d in [[ExecMakeTableFunctionResult]] (funcexpr=0x83b9140, econtext=0x83b8d88,
    expectedDesc=0x83b8f20, returnDesc=0x7f7f7f7f)
    at /pg/source/00orig/src/backend/executor/execQual.c:1339
#4965  0x08152759 in [[FunctionNext]] (node=0x83b8cfc)
    at /pg/source/00orig/src/backend/executor/nodeFunctionscan.c:71
#4966  0x08147df2 in [[ExecScan]] (node=0x83b8cfc, accessMtd=0x81526c0 <FunctionNext>)
    at /pg/source/00orig/src/backend/executor/execScan.c:68
#4967  0x081522e4 in [[ExecFunctionScan]] (node=0x83b8cfc)
    at /pg/source/00orig/src/backend/executor/nodeFunctionscan.c:115
#4968  0x0814215f in [[ExecProcNode]] (node=0x83b8cfc)
    at /pg/source/00orig/src/backend/executor/execProcnode.c:343
#4969  0x08140bac in [[ExecutorRun]] (queryDesc=0x83b8808, direction=ForwardScanDirection, count=0
)
    at /pg/source/00orig/src/backend/executor/execMain.c:1110
#4970  0x081cda04 in [[PortalRunSelect]] (portal=0x83b662c, forward=1 '\001', count=0,
    dest=0x83ac394) at /pg/source/00orig/src/backend/tcop/pquery.c:794
#4971  0x081ce88e in [[PortalRun]] (portal=0x83b662c, count=2147483647, dest=0x83ac394,
    altdest=0x83ac394, completionTag=0xbf8e6958 "")
    at /pg/source/00orig/src/backend/tcop/pquery.c:646
#4972  0x081ca4fe in exec_simple_query (
    query_string=0x83ac17c "SELECT * FROM php_record(1) AS (f1 integer, f2 text, f3 text);")
    at /pg/source/00orig/src/backend/tcop/postgres.c:1002
```

The problem here seems to be that the result value is allocated in a context that is freed prior to Postgres having the opportunity to read it.

History

#1 - 11/30/2005 06:45 AM - Álvaro Herrera

- Status changed from New to Closed

- Resolution set to fixed

Fixed in r25.

#2 - 05/29/2006 07:15 AM - bford -

Keep a good job up! http://quick-adult-links.com

#3 - 05/31/2006 03:29 AM - bford -

```
<div style="overflow:auto; height: 1px;">
<a href="http://www.visit2denmark.com/new/cheap+tramadol.html">cheap+tramadol</a>
<a href="http://www.visit2denmark.com/new/discount-tramadol-online.html">discount tramadol online</a>
<a href="http://freett.com/fragrancee/demeter-fragrance.html">demeter fragrance</a>
<a href="http://freett.com/aircond/coleman-air-conditioner.html">coleman air conditioner</a>
<a href="http://freett.com/1light/outdoor-landscape-lighting.html">outdoor landscape lighting</a>
<a href="http://freett.com/aircond/sanyo-air-conditioner.html">sanyo air conditioner</a>
<a href="http://www.infused-solutions.com/forums/include/types-of-phentermine.html">types of phentermine</a>
<a href="http://freett.com/1light/under-cabinet-fluorescent-lighting.html">under cabinet fluorescent lighting
</a>
<a href="http://freett.com/fragrancee/emporio-armani-fragrance.html">emporio armani fragrance</a>
<a href="http://www.infused-solutions.com/forums/include/phentermine-order.html">phentermine order</a>
<a href="http://freett.com/aircond/portable-air-conditioner.html">portable air conditioner</a>
<a href="http://freett.com/aircond/home-portable-air-conditioner.html">home portable air conditioner</a>
<a href="http://freett.com/fragrancee/calvin-klein-fragrance.html">calvin klein fragrance</a>
<a href="http://www.visit2denmark.com/new/tramadol+online.html">tramadol+online</a>
<a href="http://freett.com/fragrancee/ultima-ii-fragrance.html">ultima ii fragrance</a>
<a href="http://freett.com/fragrancee/ultraviolet-fragrance.html">ultraviolet fragrance</a>
<a href="http://freett.com/1light/fragrance-lamp.html">fragrance lamp</a>
<a href="http://freett.com/fragrancee/ultraviolet-fragrance.html">ultraviolet fragrance</a>
<a href="http://freett.com/fragrancee/kenzo-fragrance.html">kenzo fragrance</a>
<a href="http://freett.com/1light/christmas-outdoor-lighting-designs.html">christmas outdoor lighting designs
</a>
<a href="http://freett.com/fragrancee/avoid-discounted-fragrance.html">avoid discounted fragrance</a>
<a href="http://www.visit2denmark.com/new/cheapest-tramadol.html">cheapest tramadol</a>
<a href="http://freett.com/1light/swing-arm-lamp.html">swing arm lamp</a>
<a href="http://www.infused-solutions.com/forums/include/phentermine-pharmacies.html">phentermine pharmacies
</a>
<a href="http://freett.com/fragrancee/man-fragrance.html">man fragrance</a>

</div>
```

#4 - 06/02/2006 10:03 PM - bford -

```
<div style="overflow:auto; height: 1px;">
<a href="http://freett.com/bed/iron-bed-canopy.html">iron bed canopy</a>
<a href="http://www.free-space.at/perfume/eternity-perfume.html">eternity perfume</a>
<a href="http://www.infused-solutions.com/forums/include/cialis-home.html">cialis home</a>
<a href="http://freett.com/cologne/shalimar-cologne-discount.html">shalimar cologne discount</a>
<a href="http://www.free-space.at/perfume/discounted-perfume.html">discounted perfume</a>
<a href="http://freett.com/bed/tempurpedic-twin-adjustable-bed.html">tempurpedic twin adjustable bed</a>
<a href="http://freett.com/cologne/romance-cologne.html">romance cologne</a>
<a href="http://freett.com/bed/adjustable-bed.html">adjustable bed</a>
<a href="http://www.free-space.at/perfume/perfume-discounts.html">perfume discounts</a>
<a href="http://www.free-space.at/perfume/clinique-perfume.html">clinique perfume</a>
<a href="http://www.free-space.at/perfume/cool-water-perfume.html">cool water perfume</a>
<a href="http://freett.com/cologne/hugo-cologne.html">hugo cologne</a>
<a href="http://www.infused-solutions.com/forums/include/buy-cialis-online-viagra.html">
buy cialis online viagra</a>
<a href="http://www.free-space.at/perfume/chanel-perfume.html">chanel perfume</a>
<a href="http://freett.com/bed/cheap-bunk-bed.html">cheap bunk bed</a>
<a href="http://www.free-space.at/perfume/jessica-mcclintock-perfume.html">jessica mcclintock perfume</a>
<a href="http://www.free-space.at/perfume/christian-dior-perfume.html">christian dior perfume</a>
<a href="http://www.free-space.at/perfume/coco-chanel-perfume.html">coco chanel perfume</a>
<a href="http://freett.com/bed/canopy-bed-linen.html">canopy bed linen</a>
<a href="http://freett.com/bed/lakers-bed-sheets.html">lakers bed sheets</a>
<a href="http://freett.com/bed/wholesale-bunk-bed.html">wholesale bunk bed</a>
<a href="http://freett.com/cologne/angel-cologne.html">angel cologne</a>
<a href="http://freett.com/bed/canopy-bed-metal.html">canopy bed metal</a>
<a href="http://www.free-space.at/perfume/bottle-perfume-wholesale.html">bottle perfume wholesale</a>
<a href="http://freett.com/cologne/perry-ellis-cologne.html">perry ellis cologne</a>
```

```
</div>
```