Ivannikov ISP RAS

Svace

ANALYSIS RESULTS

Project	server
Branch	master
Snapshot	Snapshot 2024-03-26 19:56:19 +0300

Product version

3.3.2

Report creation date

27 March 2024

Table of contents

1. DEREF_AFTER_NULL

A pointer is compared to NULL (which indicates that it could have a NULL value), and then it is dereferenced.

Language	Severity	Reliability	Status	Situation
CSHARP	Critical	High	true	Quality
CXX	Critical	High	true	Quality
GO	Critical	High	true	Quality
JAVA	Major	High	true	Quality
KOTLIN	Normal	High	true	Quality

Location: /server/sql/wsrep_utils.h:114	
Function	_ZN3wsp7Address10parse_addrEPKc
Warning message	After having been compared to a NULL value at wsrep_utils.h:103, pointer 'close_bracket' is dereferenced at wsrep_utils.h:114 by calling function 'strchr'.
Комментарий	на 1249 строчке вызывается функция *inject_cond_into_where* и в нее передается результат вызова метода *copy_andor_structure(thd)* у *inj_cond*. В этот момент происходит разыменование указателя.

```
109
110  start= open_bracket + 1;
111  end= close_bracket;
112
113  /* Check for port */
114  port= strchr(close_bracket, ':');
115  if ((port != NULL) && parse_port(port + 1))
116  {
117    return;                                  /* Error: invalid
       port */
118  }
119  m_family= INET6;
```

Location: /server/sql/opt_split.cc:1249	Should fix
Function	_ZN4JOIN26inject_best_splitting_condEy
Warning message	After having been compared to a NULL value at opt_split.cc:1246, pointer 'inj_cond' is dereferenced at opt_split.cc:1249.
Комментарий	на 1249 строчке вызывается функция *inject_cond_into_where* и в нее передается результат вызова метода *copy_andor_structure(thd)* у *inj_cond*. Потенциально разыменовывается пустой указатель

```
1244      return true;
1245  }
1246  if (inj_cond)
1247    inj_cond->fix_fields(thd,0);
1248
```

```
1249  if
      (inject_cond_into_where(inj_cond->copy_andor_structure(thd)
      ))
```

```
1250    return true;
1251
1252  select_lex->uncacheable|= UNCACHEABLE_DEPENDENT_INJECTED;
1253  st_select_lex_unit *unit= select_lex->master_unit();
1254  unit->uncacheable|= UNCACHEABLE_DEPENDENT_INJECTED;
```

Location: /server/sql/item.cc:1575	Undecided
Function	_ZN10Item_field25check_vcol_func_processorEPv
Warning message	After having been compared to a NULL value at item.cc:1565, pointer 'res' is passed as 2nd parameter in call to function 'mark_unsupported_function' at item.cc:1575, where it is dereferenced at item.cc:1540.

```
1570        r|= VCOL_AUTO_INC;
1571      if (field->vcol_info &&
1572          field->vcol_info->flags &
              (VCOL_NOT_STRICTLY_DETERMINISTIC | VCOL_AUTO_INC))
1573        r|= VCOL_NON_DETERMINISTIC;
1574    }
```

```
1575    return mark_unsupported_function(field_name.str, arg, r);
```

```
1576  }
1577
1578
1579  Query_fragment::Query_fragment(THD *thd, sp_head *sphead,
1580                                 const char *start, const
                                   char *end)
```

Location: /server/sql/wsrep_mysqld.cc:2179	Undecided
Function	_Z26wsrep_prepare_keys_for_toiPKcS0_PK10TABLE_LISTPK10Alter_infoPKSt6vectorIN5wsrep3keyESaIS9_EE
Warning message	After having been compared to a NULL value at wsrep_mysqld.cc:2177, pointer 'db' is passed as 1st parameter in call to function 'wsrep_prepare_key_for_toi' at wsrep_mysqld.cc:2179, where it is dereferenced at wsrep_mysqld.cc:2139.

```
2174                                                    const
                                                        wsrep::key_arra
                                                        y *fk_tables)
```

```
2175  {
2176    wsrep::key_array ret;
2177    if (db || table)
2178    {
2179      ret.push_back(wsrep_prepare_key_for_toi(db, table,
          wsrep::key::exclusive));
2180    }
2181    for (const TABLE_LIST* table= table_list; table; table=
        table->next_global)
2182    {
2183      ret.push_back(wsrep_prepare_key_for_toi(table->db.str,
          table->table_name.str,
2184                                                    wsrep::key::exc
                                                        lusive));
```

Location: /server/sql/sql_select.cc:28246	Undecided
Function	_ZL17get_sort_by_tableP8st_orderS0_R4ListI10TABLE_LISTEy
Warning message	After having been compared to a NULL value at sql_select.cc:28245, pointer 'table' is dereferenced at sql_select.cc:28246.

```
28241    if (!map || (map & (RAND_TABLE_BIT |
         OUTER_REF_TABLE_BIT)))
28242      DBUG_RETURN(0);
28243
28244    map&= ~const_tables;
28245    while ((table= ti++) && !(map & table->table->map)) ;
28246    if (map != table->table->map)
```

```
28247      DBUG_RETURN(0);                 // More than one table
28248    DBUG_PRINT("exit",("sort by table:
         %d",table->table->tablenr));
28249    DBUG_RETURN(table->table);
28250  }
28251
```