

Novel Contributions to the field

How I broke MySQL's codebase



Industry-led research presented by



Advanced Information Security Corporation

Keeping Things Simple

ORACLE®



Advanced Information Security Corporation

Keeping Things Simple



Part I Objectives - Presentation



Chapter 1

Prelude

Chapter 2

Overview & Synopsis

Chapter 3

Zero-day Vulnerabilities



Epitome ~ A Novel Contribution

The scope of this research is to mark novelty contribution to the field.

The main objective of this research is to present zero-day vulnerabilities, breaking the codebase of the most popular and most widely used database in the world.

To directly contribute to the development and enhance the security efforts of MySQL as a product, empowering the ties and efforts of our research partner Oracle Inc. pioneering cutting-edge industry-led research with proven multivariate results.

To offer something back to the security field, to give a notion of better security for open-source users. After all, this is the beauty of open-source products and technologies.

MySQL prestige by Industry



AEROSPACE, DEFENSE

- » NASA
- » Los Alamos National Laboratory
- » US Navy
- » MORE

GOVERNMENT

- » US Navy
- » Nordrhein-Westfalen, RZ der Finanzverwaltung
- » Los Alamos National Laboratory
- » MORE

RETAIL

- » Leader Price
- » Glasses Direct
- » The Phone House Telecom GmbH
- » MORE

EDUCATION

- » College of William & Mary
- » McGraw-Hill Education
- » Universität Duisburg-Essen
- » MORE

HEALTHCARE, PHARMA

- » FairWarning
- » Celltrak Technologies
- » UCR
- » MORE

SMALL & MEDIUM BUSINESS

- » thePlatform
- » Clickability
- » MORE

FINANCIAL SERVICES

- » HypoVereinsbank
- » Shinsei Bank
- » Bank of Finland
- » MORE

MEDIA & ENTERTAINMENT

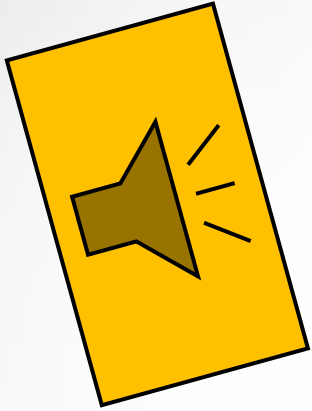
- » Televisa
- » Hachette Filipacchi Media
- » Big Fish
- » MORE

TECHNOLOGY: HARDWARE

- » Sandstorm Enterprises
- » Xceedium
- » S2 Security Corporation
- » MORE

Facebook, Google, Twitter just to name a few clients. A sample list can be seen at <http://www.mysql.com/customers/>

MySQL Milestones – The Past



Original development of MySQL by Michael Widenius and David Axmark beginning in 1994

First internal release on 23 May 1995

Version 3.19: End of 1996, from www.tcx.se

Version 3.20: January 1997

Windows version was released on 8 January 1998 for Windows 95 and NT

Version 3.21: production release 1998, from www.mysql.com

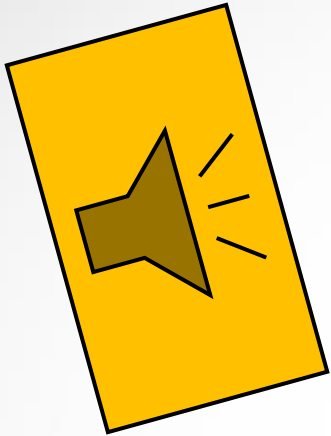
Version 3.22: alpha, beta from 1998

Version 3.23: beta from June 2000, production release 22 January 2001

Version 4.0: beta from August 2002, production release March 2003 (unions)



MySQL Milestones – The Past



Version 4.01: beta from August 2003, adopts MySQL for database tracking

Version 4.1: beta from June 2004, production release October 2004

Version 5.0: beta from March 2005, production release October 2005

Sun Microsystems acquired MySQL AB in 2008.

Version 5.1: production release 27 November 2008

Oracle acquired Sun Microsystems on 27 January 2010

MySQL Server 5.5 was generally available (as of December 2010)

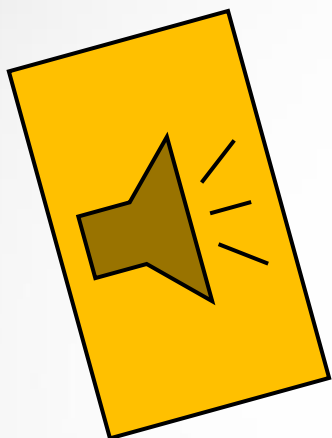
MySQL Server 6.0.11-alpha was announced^[44] on 22 May 2009

The general availability of MySQL 5.6 was announced in February 2013

The general availability of MySQL 5.7 was announced in October 2015



MySQL Milestones – Synopsis of the Past



January, 2016 – Advanced Information Security Corporation

In partnership with Oracle Inc. provided novel contributions to the security of the most popular database in the world.

MySQL Multiple Bugs Let Remote Users Access Data and Deny Service, Remote Authenticated Users Modify Data, and Local Users Gain Elevated Privileges

SecurityTracker Alert ID: 1034708

SecurityTracker URL: <http://securitytracker.com/id/1034708>

CVE Reference: [CVE-2015-7744](#), [CVE-2016-0502](#), [CVE-2016-0503](#), [CVE-2016-0504](#), [CVE-2016-0505](#), [CVE-2016-0546](#), [CVE-2016-0594](#), [CVE-2016-0595](#), [CVE-2016-0596](#), [CVE-2016-0597](#), [CVE-2016-0598](#), [CVE-2016-0599](#), [CVE-2016-0600](#), [CVE-2016-0601](#), [CVE-2016-0605](#), [CVE-2016-0606](#), [CVE-2016-0607](#), [CVE-2016-0608](#), [CVE-2016-0609](#), [CVE-2016-0610](#), [CVE-2016-0611](#), [CVE-2016-0616](#) (Links to External Site)

Date: Jan 19 2016

Impact: [Denial of service via network](#), [Disclosure of system information](#), [Disclosure of user information](#), [Modification of system information](#), [Modification of user information](#), [User access via local system](#)

Fix Available: Yes Vendor Confirmed: Yes

Version(s): 5.5.46 and prior, 5.6.27 and prior, 5.7.9

The following researchers reported these and other Oracle product vulnerabilities:

Adam Willard of Raytheon Foreground Security; Alexey Tyurin of ERPSan; Andrea Micalizzi aka rgod (via HP's Zero Day Initiative); Anonymous (via HP's Zero Day Initiative); Brandon Vincent; Cybersecurity-upv; David Litchfield of Google; Dmitry Janushkevich of Secunia Research; Fernando Russ of Onapsis; FortiGuard Labs of Fortinet, Inc.; Francois Goichon of Context Information Security; Igor Kopylenko of McAfee Database Security Research Team; Ivan Chalykin of ERPSan; Jakub Palaczynski from ING Services Polska; Karthikeyan Bhargavan, Gaetan Leurent of INRIA; Lowi Yu of [Salesforce.com](#); Luca Carettoni; Matias Mevied of Onapsis; Mike Arnold (Bruk0ut) (via HP's Zero Day Initiative); Nassim Bouali; [Nicholas Lemonias of Advanced Information Security Corporation](#); Nikita Kelesis of ERPSan; Peter Kostiuik of [Salesforce.com](#); Ryan Giobbi of American Eagle Outfitters; Sergey Gorbaty of [Salesforce.com](#); Shai Meir of McAfee Security Research; Spyridon Chatzimichail of COSMOTE - Mobile Telecommunications S.A.; Stefan Kanthak; Stephen Kost of Integrigy; Travis Emmert of [Salesforce.com](#); and Will Dormann of CERT/CC.

Impact: A remote user can partial access data on the target system.

A remote authenticated user can partially modify data on the target system.

A remote user can cause partial denial of service conditions.

A local user can obtain elevated privileges on the target system.

Solution: The vendor has issued a fix as part of the January 2016 Oracle Critical Patch Update.



Format String Vulnerability

Affected Line: 631 - ...\\..\\client\\mysqlcheck.c

Code Snippet:

```
sprintf(qbuf, "RENAME TABLE `'%s` TO  
`'%s`", name, name + 9)
```



Format String Vulnerability

Affected Line: 644

...\client\mysqlcheck.c

Code Snippet

```
sprintf(qbuf, "ALTER DATABASE `%s`  
UPGRADE DATA DIRECTORY NAME",  
name);
```

Big Game Hunting – Zeroday disclosure



Format String Vulnerability

Affected Line: 754 -
..\..\client\mysqlcheck.c

Code Snippet:
query_length= sprintf(query, "%s
TABLE %s %s", op, tables, options);

Big Game Hunting – Zeroday disclosure



Buffer Overflow Vulnerability

Affected Line: 847 -
..\..\client\mysqlcheck.c

Code Snippet:
`strcpy(prev_alter, alter_txt);`



Integer Overflow / Wraparound Issue

Affected Line: 882 ../../client/mysqldump.c

Code Snippet:

argument, (uint) strlen(argument),



Buffer overflow / Non-Termination of overflowed buffers

Affected Line:1176 -
..\..\client\mysqldump.c

Code Snippet:
`strncpy(db_cl_name, db_cl_row[0],
db_cl_size);`



Format String Issue

Affected Line: 5543

..\..\client\mysqldump.c

Code Snippet:

```
sprintf(insert_pat,"SET  
SQL_QUOTE_SHOW_CREATE=%d",
```

Big Game Hunting – Zeroday disclosure



Heap Overflow due to bad malloc

Affected Line: 3364

..\..\client\mysqldump.c

Code Snippet

```
static char *alloc_query_str(ulong size)
{
    char *query;

    if (!(query= (char*) my_malloc(size,
MYF(MY_WME))))
        die(EX_MYSQLERR, "Couldn't allocate a
query string.");
    return query;
}
```


Big Game Hunting – Zeroday disclosure



Integer Overflow / Wraparound

Affected Line : 549

..\..\client\mysqlshow.c

Code Snippet:

```
printf("Database: %s",db);
```

```
if (table)
```

```
    printf(" Wildcard: %s",table);
```

```
    putchar('\n');
```

```
header="Tables";
```

```
head_length=(uint) strlen(header);
```

```
field=mysql_fetch_field(result);
```

```
if (head_length < field->max_length)
```

```
    head_length=field->max_length;
```

Big Game Hunting – Zeroday disclosure



Integer Overflow

Affected Line: Line: 65
..\..\extra\yassl\src\log.cpp

Code Snippet:

```
time_t clicks = time(0);  
char timeStr[32];
```

```
// get rid of newline  
strncpy(timeStr, ctime(&clicks),  
sizeof(timeStr));  
unsigned int len = strlen(timeStr);  
timeStr[len - 1] = 0;
```

Big Game Hunting – Zeroday disclosure



Memory Corruption

Affected Line: 140 -

..\plugin\innodb_memcache
d\daemon_memcached\utili
ties\engine_loader.c

Code Snippet:

```
for (int ii = 0; ii < info-  
>num_features; ++ii) {  
    if (info-  
>features[ii].description != NULL)  
{  
        nw = snprintf(message  
+ offset, sizeof(message) - offset,  
                        "%s%s",  
comma ? ", " : "",  
                        info-  
>features[ii].description);
```

Big Game Hunting – Zeroday disclosure



Buffer Overflow / Memory Mismanagement

Affected Line: 1748

..\plugin\innodb_memcached\innodb_memcache\src\innodb_engine.c

Code Snippet:

memcpy(c_value, int_buf, int_len);

Big Game Hunting – Zeroday disclosure



Buffer Overflow

Affected Line: 166

..\mysql\mysql-5.6.24\regex\split.c

Code Snippet:

(void) strcpy(buf, argv[1]);



ORACLE

(References)

[1] Oracle Critical Patch Update - July 2016. 2016. *Oracle Critical Patch Update - July 2016*. [ONLINE] Available at: <http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html>.

[2] Threatpost | The first stop for security news. 2016. *Oracle Fixes 276 Vulnerabilities in July Critical Patch Update* | Threatpost | The first stop for security news. [ONLINE] Available at: <https://threatpost.com/oracle-patches-record-276-vulnerabilities-with-july-critical-patch-update/119373/>.



Advanced Information Security Corporation

Keeping Things Simple

Author: Nicholas Lemonias CEO

Presentation Date:
19/7/2016