Novel Contributions to the field
How I broke MySQL's code-base (Part 2)

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 ~ Novel contribution

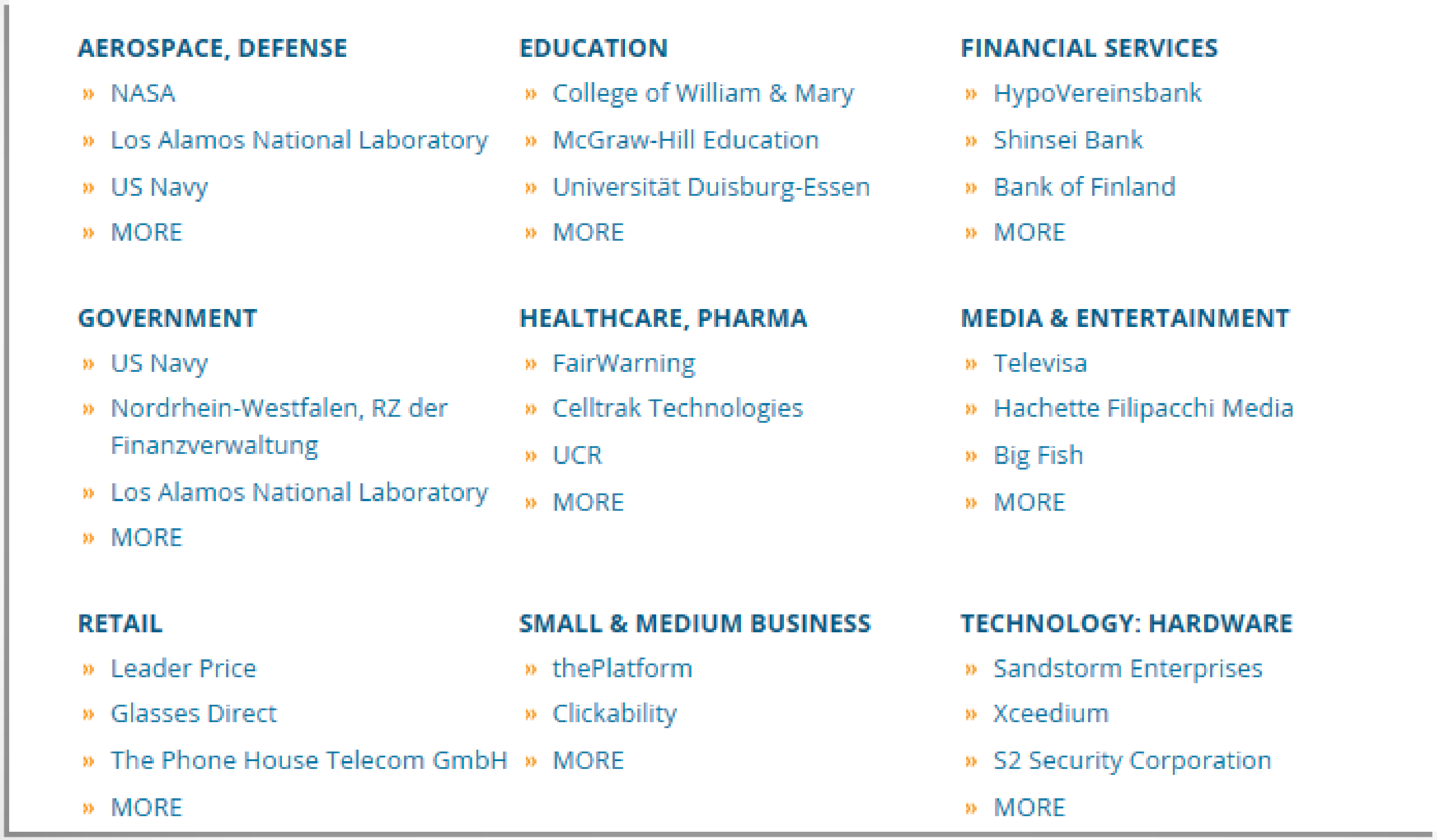
The scope of this research is to mark novelty contribution to the field.

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

EDUCATION

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

FINANCIAL SERVICES

- HypoVereinsbank
- Shinsei Bank
- Bank of Finland
- MORE

GOVERNMENT

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

HEALTHCARE, PHARMA

- FairWarning
- Celltrak Technologies
- UCR
- MORE

MEDIA & ENTERTAINMENT

- Televisa
- Hachette Filipacchi Media
- Big Fish
- MORE

RETAIL

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

SMALL & MEDIUM BUSINESS

- thePlatform
- Clickability
- MORE

TECHNOLOGY: HARDWARE

- Sandstorm Enterprises
- Xceedium
- S2 Security Corporation
- MORE

Facebook, Google, Twitter just to name a few clients. A sample list can be found 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

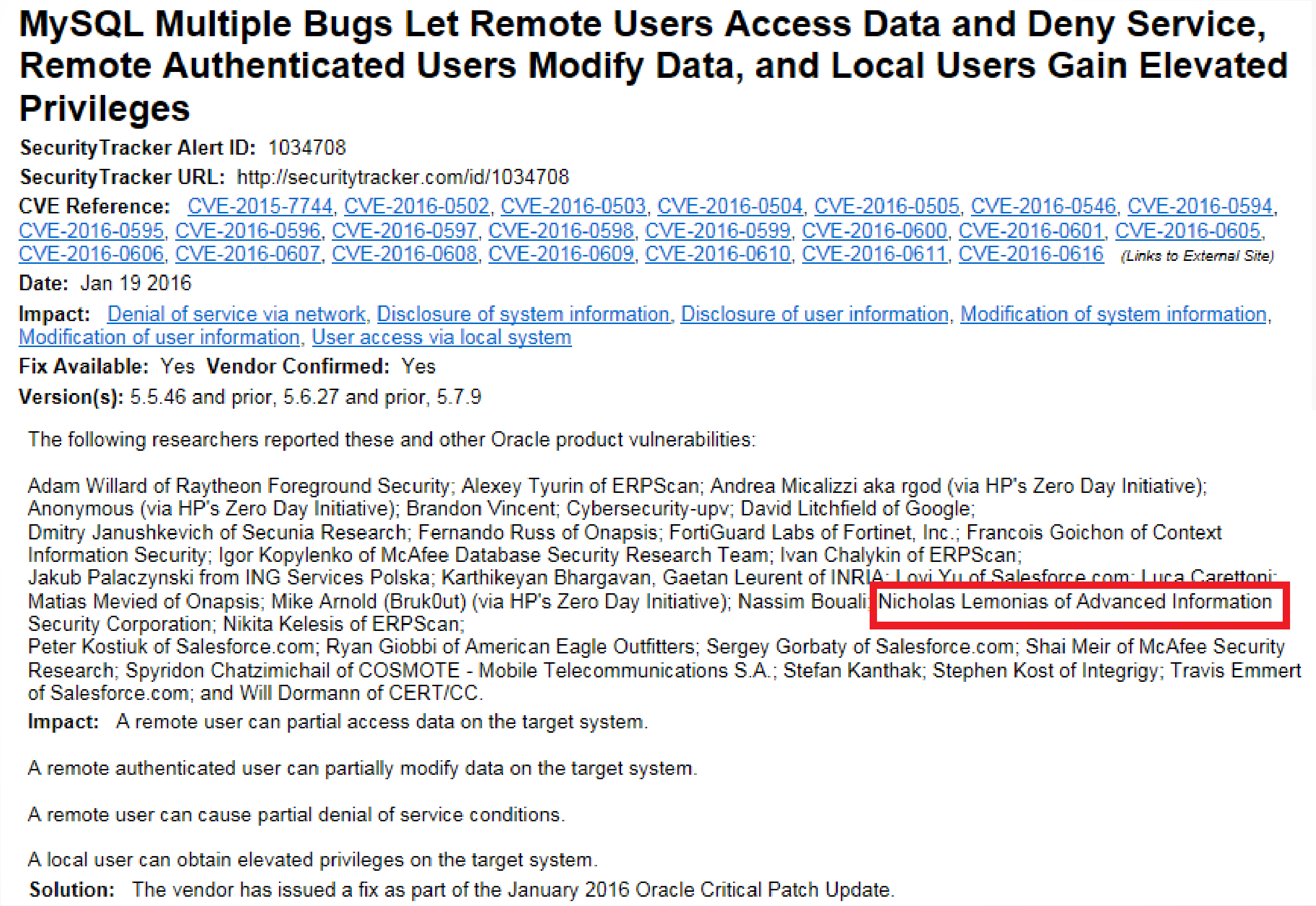
MySQL Server 6.0.11-alpha was announced[44] on 22 May 2009

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 ERPScan; 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 ERPScan; Jakub Palaczynski from ING Services Polska; Karthikeyan Bhargavan, Gaetan Leurent of INRIA; Lovi 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 ERPScan; Peter Kostiuk 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.

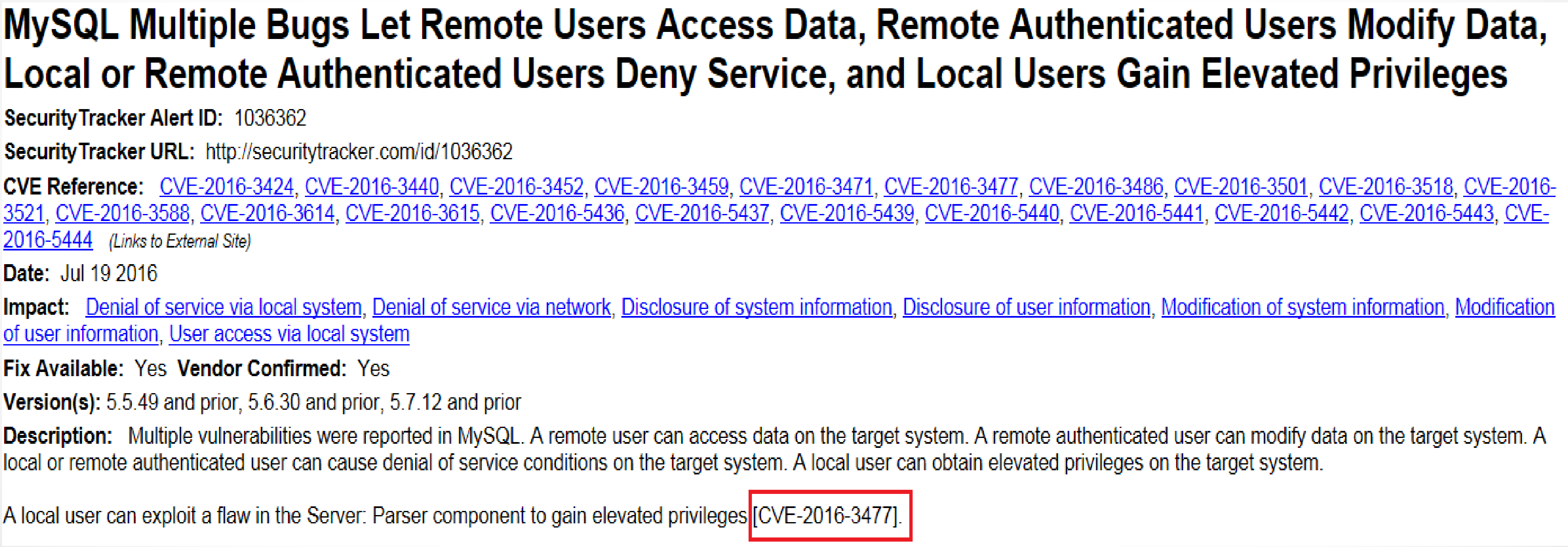
A remote user can cause partial denial of service conditions.

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.

MySQL milestones -Synopsis of the past

July, 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, Remote Authenticated Users Modify Data, Local or Remote Authenticated Users Deny Service, and Local Users Gain Elevated Privileges

SecurityTracker Alert ID: 1036362

SecurityTracker URL: http://securitytracker.com/id/1036362

CVE Reference: CVE-2016-3424, CVE-2016-3440, CVE-2016-3452, CVE-2016-3459, CVE-2016-3471, CVE-2016-3477, CVE-2016-3486, CVE-2016-3501, CVE-2016-3518, CVE-2016-3521, CVE-2016-3588, CVE-2016-3614, CVE-2016-3615, CVE-2016-5436, CVE-2016-5437, CVE-2016-5439, CVE-2016-5440, CVE-2016-5441, CVE-2016-5442, CVE-2016-5443, CVE-2016-5444 *(Links to External Site)*

Date: Jul 19 2016

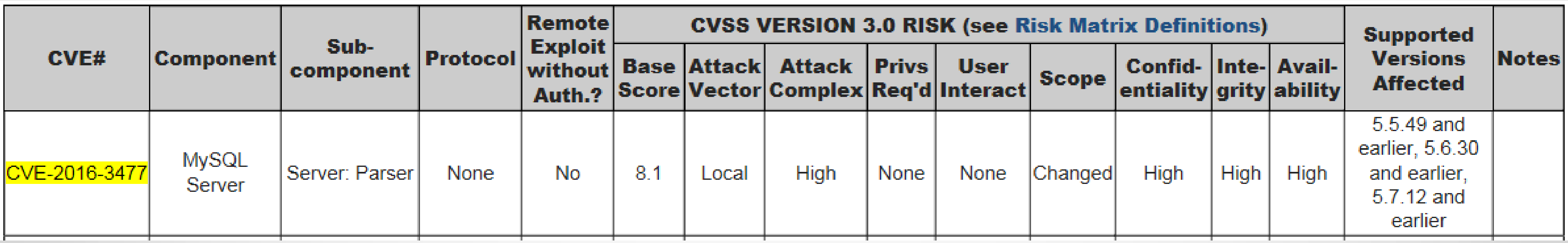
Impact: Denial of service via local system, Denial of service via network, Disclosure of system information, Disclosure of user information, Modification of system information, Modification of user information, User access via local system

Fix Available: Yes **Vendor Confirmed:** Yes

Version(s): 5.5.49 and prior, 5.6.30 and prior, 5.7.12 and prior

Description: Multiple vulnerabilities were reported in MySQL. A remote user can access data on the target system. A remote authenticated user can modify data on the target system. A local or remote authenticated user can cause denial of service conditions on the target system. A local user can obtain elevated privileges on the target system.

A local user can exploit a flaw in the Server: Parser component to gain elevated privileges [CVE-2016-3477].

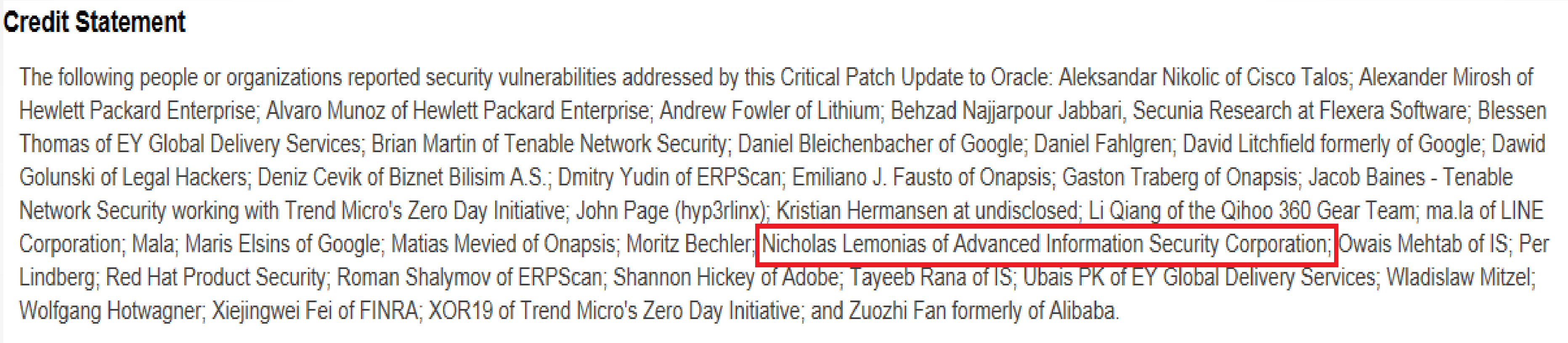


CVE#	Component	Sub-component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK (see Risk Matrix Definitions)									Supported Versions Affected	Notes
					Base Score	Attack Vector	Attack Complex	Privs Req'd	User Interact	Scope	Confid-entiality	Inte-grity	Avail-ability		
CVE-2016-3477	MySQL Server	Server: Parser	None	No	8.1	Local	High	None	None	Changed	High	High	High	5.5.49 and earlier, 5.6.30 and earlier, 5.7.12 and earlier	

Chapter 2

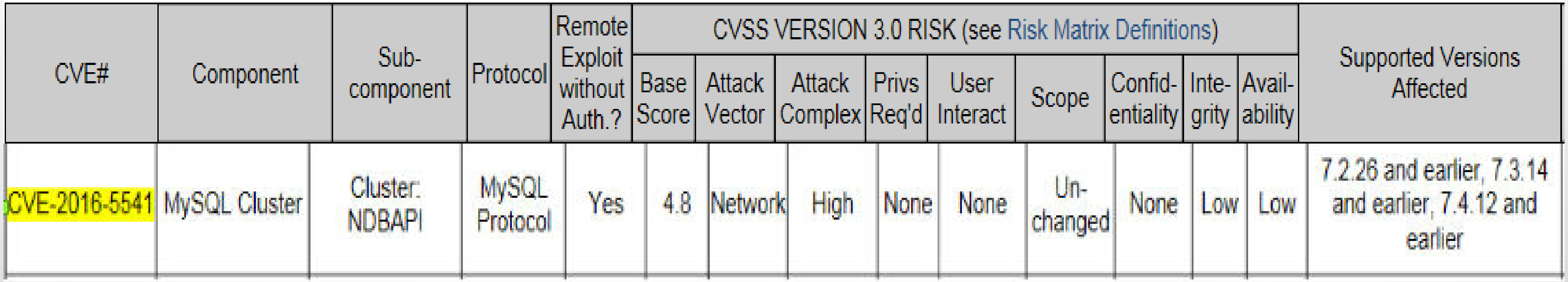
New year, new improvements!

January, 2017 – Advanced Information Security Corporation
In partnership with Oracle Inc. provided novel contributions to the security of the most popular database in the world.



Credit Statement

The following people or organizations reported security vulnerabilities addressed by this Critical Patch Update to Oracle: Aleksandar Nikolic of Cisco Talos; Alexander Mirosh of Hewlett Packard Enterprise; Alvaro Munoz of Hewlett Packard Enterprise; Andrew Fowler of Lithium; Behzad Najjarpour Jabbari, Secunia Research at Flexera Software; Blessen Thomas of EY Global Delivery Services; Brian Martin of Tenable Network Security; Daniel Bleichenbacher of Google; Daniel Fahlgren; David Litchfield formerly of Google; Dawid Golunski of Legal Hackers; Deniz Cevik of Biznet Bilisim A.S.; Dmitry Yudin of ERPScan; Emiliano J. Fausto of Onapsis; Gaston Traberg of Onapsis; Jacob Baines - Tenable Network Security working with Trend Micro's Zero Day Initiative; John Page (hyp3rlinx); Kristian Hermansen at undisclosed; Li Qiang of the Qihoo 360 Gear Team; ma.la of LINE Corporation; Mala; Maris Elsins of Google; Matias Mevied of Onapsis; Moritz Bechler; Nicholas Lemonias of Advanced Information Security Corporation; Owais Mehtab of IS; Per Lindberg; Red Hat Product Security; Roman Shalymov of ERPScan; Shannon Hickey of Adobe; Tayeeb Rana of IS; Ubais PK of EY Global Delivery Services; Wladislaw Mitzel; Wolfgang Hotwagner; Xiejingwei Fei of FINRA; XOR19 of Trend Micro's Zero Day Initiative; and Zuozhi Fan formerly of Alibaba.



CVE#	Component	Sub-component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK (see Risk Matrix Definitions)									Supported Versions Affected
					Base Score	Attack Vector	Attack Complex	Privs Req'd	User Interact	Scope	Confidentiality	Integrity	Availability	
CVE-2016-5541	MySQL Cluster	Cluster: NDBAPI	MySQL Protocol	Yes	4.8	Network	High	None	None	Unchanged	None	Low	Low	7.2.26 and earlier, 7.3.14 and earlier, 7.4.12 and earlier

Big Game Hunting – MySQL 0days

1. MySQL Cluster ‘NDBAPI’ / Remote Buffer Overflow

Affected Line:

..\storage\ndb\src\ndbapi\NdbBlob.cpp: 1518
..\sql\ha_ndbcluster_binlog.cc:445
..\storage\ndb\tools\ndb_lib_move_data.cpp:688

Code Snippet:

```
memcpy(buf, thePartBuf.data, len);
```

The source-code lacked controls in the code paths leading to ‘readDataPrivate’ which is susceptible to buffer overflow conditions. Passed size of variable buf instead of passing UINT_MAX as the "bytes" argument.

Big Game Hunting – MySQL 0days

MySQL Cluster / Remote Buffer Overflow

January, 2017 Patch Update

Oracle Inc. provided security fixes in code paths leading to 'readDataPrivate' to prevent buffer overflows.

(i) sql/ha_ndbcluster_binlog.cc, at line 445: Passed size of variable buf instead of passing UINT_MAX as the "bytes" argument.

(ii) Added an assert in storage/ndb/tools/ndb_lib_move_data.cpp, line 688 to make sure "length1" is lesser than or equal to the buffer size.

Big Game Hunting – Zeroday disclosure

2. Buffer Overflow

Affected Line: 86
..\storage\ndb\src\common\portlib\NdbConfig.c

Code Snippet

```
strcat(buf, tmp_buf);
```

Oracle Mitigation

Added an assert(len > 0) to prevent overflow of buffers.

Big Game Hunting – Zeroday disclosure

3. Memory Mismanagement

Affected Line: 40

..\storage\ndb\src\common\portlib\NdbMem.c

Oracle Mitigation:
Called ndb_end() function in places where controls were missing.

ORACLE

(References)

[1] Oracle Critical Patch Update - January 2017. 2017. *Oracle Critical Patch Update - January 2017*. [ONLINE] Available at: http://www.oracle.com/technetwork/security-advisory/cpujan2017-2881727.html

Advanced Information Security Corporation

Keeping Things Simple

Author: Nicholas Lemonias

Presentation Date:
17/01/2017