

mongodb vNone6378/TCP, 29 9 CVE.

CVE

CVE-2013-4650

.....

MongoDB 2.4.x before 2.4.5 and 2.5.x before 2.5.1 allows remote authenticated users to obtain internal system privileges by leveraging a username of __system in an arbitrary database.

..... .. 2

..... **6.5****MEDIUM**

..... ..

..... .. CVE, Python CGIHTTP
.. CVE-2013-4650.,

... .. CVE-2014-4650,
python27 python-pip: python27, ..
..... ..

..... ..;

- 1
- 2 (PoLP) -
- 3
- 4

CVE-2017-15535

.....

MongoDB 3.4.x before 3.4.10, and 3.5.x-development, has a disabled-by-default configuration setting, networkMessageCompressors (aka wire protocol compression), which exposes a vulnerability when enabled that could be exploited by a malicious attacker to deny service or modify memory.

..... .. 2

..... **6.4****MEDIUM**

..... .. 3

..... **9.1****CRITICAL**

..... ..

..... .. CVE-2017-15535 · MongoDB 3.4.x · 3.4.10 · 3.5.x-development
....., 3.4.10 · 3.5.x "networkMessageCompressors",
..... "networkMessageCompressors",
..... ..

CVE-2017-14227

.....

In MongoDB libbson 1.7.0, the bson_iter_codewscope function in bson-iter.c miscalculates a bson_utf8_validate length argument, which allows remote attackers to cause a denial of service (heap-based buffer over-read in the bson_utf8_validate function in bson-utf8.c), as demonstrated by bson-to-json.c.

..... .. 2

..... ~~5.5~~.....**MEDIUM**

..... .. 3

..... ~~7.5~~.....**HIGH**

..... ..

CVE-2017-14227

CVE-2016-3104

.....

mongod in MongoDB 2.6, when using 2.4-style users, and 2.4 allow remote attackers to cause a denial of service (memory consumption and process termination) by leveraging in-memory database representation when authenticating against a non-existent database.

..... .. 2

..... ~~5.5~~.....**MEDIUM**

..... .. 3

..... ~~7.5~~.....**HIGH**

..... ..

..... CVE-2016-3104 MongoDB 2.6 · 2.4 2.4.,

....., MongoDB.,

- 1 MongoDB,
- 2 MongoDB.,
- 3 MongoDB

....., MongoDB:

- ... MongoDB 2.6<http://docs.mongodb.org/v2.6/release-notes/#security>
 - ... MongoDB 2.4<http://docs.mongodb.org/v2.4/release-notes/#security>
-

CVE-2016-6494

.....

The client in MongoDB uses world-readable permissions on .dbshell history files, which might allow local users to obtain sensitive information by reading these files.

..... 2

..... **2.1** **LOW**

..... 3

..... **5.5** **MEDIUM**

.....

....., **CVE-2016-6449** **dbshell** **MongoDB**
....., **MongoDB**,

.....;

1 **dbshell** **/home/MongoDB**
2 **dbshell**, **dbshell**

chmod 600 .dbshell*

....., (.....).

3, **ls -l**

-rw----- 1 mongodb mongodb 1234 7 10:00 .dbshell_history

..... **"rw-----"**,

.....,

CVE-2014-3971

.....

The CmdAuthenticate::_authenticateX509 function in db/commands/authentication_commands.cpp in mongod in MongoDB 2.6.x before 2.6.2 allows remote attackers to cause a denial of service (daemon crash) by attempting authentication with an invalid X.509 client certificate.

..... 2

..... **5** **MEDIUM**

.....

..... (NVD), **CVE-2014-3971** **MongoDB**

CmdAuthenticate::_authenticateX509 db/commands/authentication_commands.cpp

MongoDB 2.6.x .. 2.6.2, (.....),

....., **MongoDB** .. 2.6.2,

CVE-2013-2132

.....

bson/_cbsonmodule.c in the mongo-python-driver (aka. pymongo) before 2.5.2, as used in MongoDB, allows context-dependent attackers to cause a denial of service (NULL pointer dereference and crash) via vectors related to decoding of an "invalid DBRef."

..... 2

..... **4.3** **MEDIUM**

.....

..... CVE-2013-1892, mongo-python-driver,
pymongo, 2.5.2 DBRef, (....).

CVE-2013-1892

.....

MongoDB before 2.0.9 and 2.2.x before 2.2.4 does not properly validate requests to the nativeHelper function in SpiderMonkey, which allows remote authenticated users to cause a denial of service (invalid memory access and server crash) or execute arbitrary code via a crafted memory address in the first argument.

..... 2

..... **6** **MEDIUM**

.....

....., - CVE-2013-1892, MongoDB .. 2.0.9 .. 2.2.x .. 2.2.4, ".....
nativeHelper" .. SpiderMonkey, (.....)
.....).

.....;

- 1 **MongoDB:** MongoDB .. 2.0.9 .. 2.0 .. 2.2.4 .. 2.2.
..... <https://www.mongodb.org/> ..
 - 2 !.....
 - 3 !.....
 - 4 !.....
 - 5 !.....
-

CVE-2013-3969

.....

The find prototype in scripting/engine_v8.h in MongoDB 2.4.0 through 2.4.4 allows remote authenticated users to cause a denial of service (uninitialized pointer dereference and server crash) or possibly execute arbitrary code via an invalid RefDB object.

..... 2

..... **6.5** **MEDIUM**

.....

....., CVE-2013-3969 .. MongoDB 2.4.x:

- 1MongoDB MongoDB 2.4.5 MongoDB 2.6.0
2.6.0
<https://www.mongodb.com/try/download/community>.
- 2:....., MongoDB.
<http://docs.mongodb.org/v2.4/tutorial/install-mongodb-on-ubuntu/> ·
.....;
- 3! MongoDB
.....,
- 4; MongoDB x.509, SCrypt ... SCRAM-SHA-1.
..... MongoDB
<https://docs.mongodb.com/manual/core/authentication/>.
- 5:..... MongoDB.
.....
- 6:....., MongoDB.
openwall.com/lists/oss-security/ · JIRA,-9878.

.....,
