ZABBIX SUMMIT ONLINE /2020

"ZABBIX & SECURITY MAKING ZABBIX MUCH BETTER"

Luiz Sales

CEO

ServiceMonit BRAZIL

About

- Luiz Sales
- Managing Partner at ServiceMonit
- Specialist and Professional Zabbix
- Zabbix user since 2001, Technology Enthusiast and Lover of the Impossible

- luiz.sales@servicemonit.com.br
- https://github.com/lsa1es/
- https://www.linkedin.com/in/lsa1es/

ServiceMonit

Is Zabbix secure?

Service-Monit

How can something that allows a plaintext password be secure?

Vulnerability

Vulnerability

/etc/zabbix/zabbix_server.conf

DBHost=192.168.3.4
DBName=zabbix
DBUser=zabbix
DBPassword=ZabbixTheBestMonit

Service-Monit

Vulnerability

/etc/zabbix/zabbix_server.conf

DBHost=192.168.3.4
DBName=zabbix
DBUser=zabbix
DBPassword=ZabbixTheBestMonit

Service-Monit

How to solve?

Function in C

```
int Encrypt(DB_PARAMS) {

#include <stdio.h>

int main( int argc, char *argv[] )  {
   int i, x;
   for(i = 0; (i < 100 && argv[1][i] != '\0'); i++)
   argv[1][i] = argv[1][i] - 3; //the key for encryption is 3 that is subtracted to ASCII value
   printf("\nEncrypted string: %s\n", argv[1]);
  }
}
```

Function in C

```
int Decrypt(DB_PARAMS) {

#include <stdio.h>

int main( int argc, char *argv[] )  {
   int i, x;
   for(i = 0; (i < 100 && argv[1][i] != '\0'); i++)
   argv[1][i] = argv[1][i] + 3; //the key for encryption is 3 that is subtracted to ASCII value
   printf("\nEncrypted string: %s\n", argv[1]);
  }
}
```

Function in C (src/libs/zbxdb/db.c)

```
// Decrypt lsales
char decrypt( int argc, char *argv[]  )  {



   int i;
   for(i = 0; (i < 100 && argv[1][i] != '\0'); i++)
   argv[1][i] = argv[1][i] - 3; //the key for encryption is 3 that is subtracted to ASCII value
   printf("%s", argv[1]);



}

int     zbx_db_connect(char *host, char *user, char *password, char *dbname, char *dbschema, char *dbsocket, int port)
```

Function in C (src/libs/zbxdbhigh/db.c)

```
int     DBconnect(int flag)
{ int     err;
        zabbix_log(LOG_LEVEL_DEBUG, "In %s() flag:%d", __func__, flag);
        while (ZBX_DB_OK != (err = zbx_db_connect(decrypt(CONFIG_DBHOST), decrypt(CONFIG_DBUSER),
decrypt(CONFIG_DBPASSWORD),decrypt(CONFIG_DBNAME), CONFIG_DBSCHEMA, CONFIG_DBSOCKET,
decrypt(CONFIG_DBPORT))))
        { if (ZBX_DB_CONNECT_ONCE == flag)
                        break;
                if (ZBX_DB_FAIL == err || ZBX_DB_CONNECT_EXIT == flag)
                { zabbix_log(LOG_LEVEL_CRIT, "Cannot connect to the database. Exiting...");
                        exit(EXIT_FAILURE); }
                zabbix_log(LOG_LEVEL_ERR, "database is down: reconnecting in %d seconds", ZBX_DB_WAIT_DOWN);
                connection_failure = 1;
                zbx_sleep(ZBX_DB_WAIT_DOWN); }
        if (0 != connection_failure)
        { zabbix_log(LOG_LEVEL_ERR, "database connection re-established");
                connection_failure = 0; }
```

CRASH!

CRASH!

```
[root@node03 zabbix-4.4.6]# cat /tmp/zabbix_server.log
 27439:20201018:231117.705 Starting Zabbix Server. Zabbix 4.4.6 (revision 8cc702429d).
 27439:20201018:231117.705 ****** Enabled features ******

27439:20201018:231117.705 using configuration file: /usr/local/summit2020/etc/zabbix_server.conf
 27439:20201018:231117.706 Got signal [signal:11(SIGSEGV),reason:1,refaddr:0x8]. Crashing ...
 27439:20201018:231117.706 ====== Fatal information: ======
 27439:20201018:231117.706 Program counter: 0x55a34f

27439:20201018:231117.707 7: /usr/local/summit2020/sbin/zabbix_server(decrypt+0x1f) [0x55a34f]
 27439:20201018:231117.707 6: /usr/local/summit2020/sbin/zabbix_server(DBconnect+0x81) [0x546ba1]
 27439:20201018:231117.708 5: /usr/local/summit2020/sbin/zabbix_server(zbx_db_get_database_type+0x15) [0x549e95]

27439:20201018:231117.713 Please consider attaching a disassembly listing to your bug report.
 27439:20201018:231117.713 This listing can be produced with, e.g., objdump -DSswx zabbix_server.
```

How can you help?

Support.Zabbix.com
ZBX-11287

Who does not have a dog,
hunts with a cat.

Service-Monit

HANDS-ON

Database Name

./zabbix_server.sh crypt zabbix

U2FsdGVkX1+HWDaJdPMhKMljxcxSO3//JDsNZtRu/nI=

Database Password

./zabbix_server.sh crypt ZabbixTheBestMonit

U2FsdGVkX18M8KHS/h1J4VXAnSfqzIw8160rKO0RnF2Kz2ofatG9GWRobO7VLYzY

Service-Monit

HANDS-ON

/etc/zabbix/zabbix_server.conf

DBHost=192.168.0.1
DBName=zabbix
DBUser=ZbxUser
DBPassword=ZabbixTheBestMonit

/etc/zabbix/zabbix_server.conf

DBHost=U2FsdGVkX1/z22MUcVvrNv1Elqyaon0qfY2g53HdNBM=
DBName=U2FsdGVkX1+HWDaJdPMhKMljxcxSO3//JDsNZtRu/nI=
DBUser=U2FsdGVkX1897fZN1wlgEWlJ8gP7EdsZ0gFOspCrj1s=
DBPassword=U2FsdGVkX18M8KHS/h1J4VXAnSfqzIw8160rKO0RnF2Kz2ofatG9GWRobO7VLYzY

Service-Monit

HANDS-ON -> Source Code

zabbix_server

```
crypt() {
        echo "$2" | openssl enc -aes-128-cbc -a -salt -pass pass:wtf
}
decrypt() {
        echo "$2"  |  openssl enc -aes-128-cbc -a -d -salt -pass pass:wtf
}
```

HANDS-ON -> Source Code

zabbix_server

```
TMPF=$(mktemp)
BIN_FILE=$(find / -name zabbix_server  | grep sbin)
CHK_FILE=$(file $BIN_FILE | grep "shell script" | wc -l)
if [ $CHK_FILE -eq "1" ]; then
        CNF_FILE=$(`echo $BIN_FILE`".old" -h | grep default: | awk -F\" '{print $2}')
        cat $CNF_FILE | grep -v ^"#" | awk 'NF>0' > $TMPF
        for q in `cat $TMPF | grep =U2F`
        do
                param=$(echo $q | awk -F\= '{print $1}')
                crypt=$(echo $q | awk -F\= '{print $2"="$3}')
                decrypt=$($0 decrypt $crypt)
                regexq=$(echo $q | sed 's/\//\\\//g')
                sed -i "s/$regexq/$param=$decrypt/g" $TMPF
        done
        #cat $TMPF | grep -v ^"#" | awk 'NF>0'
        $BIN_FILE".old" -c $TMPF $1 $2 $3 $4 $5 $6 $7 $8 $9 $10 | sed 's/.old//g'
        rm -rf $TMPF
```

Service-Monit

HANDS-ON -> Frontend

./zabbix_server –V

zabbix_server (Zabbix) 4.4.6
Revision 8cc702429d 21 February 2020, compilation time: Mar 2 2020 17:32:13

Copyright (C) 2020 Zabbix SIA
License GPLv2+: GNU GPL version 2 or later <http://gnu.org/licenses/gpl.html>.
This is free software: you are free to change and redistribute it according to
the license. There is NO WARRANTY, to the extent permitted by law.

Service-Monit

HANDS-ON -> Backend

```
++ mktemp
+ TMPF=/tmp/tmp.MKnJMQRnYB
++ find / -name zabbix_server
++ grep sbin
+ BIN_FILE=/opt/summit/sbin/zabbix_server
++ file /opt/summit/sbin/zabbix_server
++ grep 'shell script'
++ wc -l
+ CHK_FILE=1
+ '[' 1 -eq 1 ']'
++ grep default:
++ awk '-F"' '{print $2}'
+++ echo /opt/summit/sbin/zabbix_server
++ /opt/summit/sbin/zabbix_server.old -h
+ CNF_FILE=/opt/summit/etc/zabbix_server.conf
+ cat /opt/summit/etc/zabbix_server.conf
+ grep -v '^#'
+ awk 'NF>0'
++ cat /tmp/tmp.MKnJMQRnYB
++ grep =U2F
+ for q in '`cat $TMPF | grep =U2F`'
++ /opt/summit/sbin/zabbix_server decrypt
U2FsdGVkX1/w3lLVkUyIDeqXownGdAsZ9ucmJ6ttTVYwgvFoi4e/nFKgbMjTygdx=
+ decrypt=ZabbixTheBestMonit
DBPassword=U2FsdGVkX1/w3lLVkUyIDeqXownGdAsZ9ucmJ6ttTVYwgvFoi4e/n
FKgbMjTygdx
+ sed -i
's/DBPassword=U2FsdGVkX1\/w3lLVkUyIDeqXownGdAsZ9ucmJ6ttTVYwgvFoi4
e\/nFKgbMjTygdx/DBPassword=ZabbixTheBestMonit/g'
/tmp/tmp.MKnJMQRnYB
+ sed s/.old//g
+ /opt/summit/sbin/zabbix_server.old -c /tmp/tmp.MKnJMQRnYB -V
zabbix_server (Zabbix) 4.4.6
Revision 8cc702429d 21 February 2020, compilation time: Oct 19 2020
01:51:31
Copyright (C) 2020 Zabbix SIA
License GPLv2+: GNU GPL version 2 or later
<http://gnu.org/licenses/gpl.html>.
This is free software: you are free to change and redistribute it according to
the license. There is NO WARRANTY, to the extent permitted by law.
```

ServiceMonit

How to implement

HOW TO IMPLEMENT

Download File:

https://github.com/lsa1es/Press/Summit/2020/zabbix_server.sh

 # zabbix_server .sh install

Service-Monit

That is it!

Thank you!

Service-Monit