huntr

Improper Authorization in saleor/saleor

0

✓ Valid Reported on Jan 3rd 2022

Title

GraphQL traversal due to missing permission checks

Description

`orders` and `customers` fields allow to access each other via nodes edges. However, connections don't check user's permissions, which allows, for instance, a staff with just `Customers` permissions get full information about the order, though direct access is forbidden.

Steps to reproduce

I will use a "Staff without `Orders` permission" scenario

1. As an admin create a staff, add this account to a group with just `Customers` permission.
2. As a created staff observe that direct access to the orders is not allowed:

```
{
  "query":"{ orders(first: 10) { edges { node { id } } } }"
}
```

This `POST` query to `http://localhost:8000/graphql/` returns `You do not have permission to perform this action`.

3. Go to a page of any customer with at least one order and note that UI shows `Recent orders` with just "No. of Order", "Date", "Status" and "Total" fields. However, if you try to see the full information about an order and click on it , you'll get `Ooops!... Something's missing` , as you don't have enough permissions.

Now run this query and receive full information about all orders:

```
{
"query":"{ customers(first: 10) { edges { node { firstName,
}
```

The most interesting field here is definitely `lines` , as it completely leaks the order.

Possible remediation

Though some fields on `orders` must be visible to a staff with only `Customers` permission to see the brief info about the last orders, an access to such fields as `lines` should be restricted.

Impact

This vulnerability is capable of leaking customer's private information.

CVE
CVE-2022-0932
(Published)

Vulnerability Type
CWE-285: Improper Authorization

Severity
Medium (6.5)

Visibility
Public

Status
Fixed

Found by

Scaramouche
@scara31
unranked

This report was seen 436 times.

We are processing your report and will contact the **saleor** team within 24 hours. a year ago

We have contacted a member of the **saleor** team and are waiting to hear b

Chat with us

We have sent a follow up to the **saleor** team. We will try again in 7 days. a year ago

We have sent a second follow up to the **saleor** team. We will try again in 10 days. 10 months ago

We have sent a third and final follow up to the **saleor** team. This report is now considered stale. 10 months ago

A **saleor/saleor** maintainer validated this vulnerability 10 months ago

Scaramouche has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

We have sent a fix follow up to the **saleor** team. We will try again in 7 days. 10 months ago

We have sent a second fix follow up to the **saleor** team. We will try again in 10 days. 10 months ago

We have sent a third and final fix follow up to the **saleor** team. This report is now considered stale. 9 months ago

Marcin Gębala marked this as fixed in **3.1.2** with commit **521dfd** 9 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Scaramouche 9 months ago Researcher

Greets, hope you are well and will be able to see this comment. Are you not against assigning a CVE as a maintainer? Huntr will do it all automatically with your agreement. Thanks for the reply in advance!

Scaramouche 9 months ago Researcher

@admin Hey, sorry for the ping, could you please assign a CVE for this one if maintainer doesn't mind it?

Jamie Slome 9 months ago Admin

Absolutely, we can assign a CVE for this. Let me just check in with the maintainer to confirm 😊

Jamie Slome 9 months ago Admin

Left a comment for the maintainer on the commit here.

Scaramouche 9 months ago Researcher

@admin Thanks, Jamie, really appreciate it!

Patryk Zawadzki 9 months ago Maintainer

Please go ahead with the CVE assignment 😄

Jamie Slome 9 months ago Admin

Sorted!

Scaramouche 9 months ago Researcher

Amazing, thank you both, gentlemen😁

Sign in to join this conversation