CVE-2021-28661 Default GraphQL permission checker not inherited by query subclass

Severity:
Low (? (https://docs.silverstripe.org/en/contributing/release_process/#security-releases))
Identifier:
CVE-2021-28661
Versions Affected:
silverstripe/graphql: ^3.0.0
Versions Fixed:
silverstripe/graphql: ^3.5.2, silverstripe/graphql: ^3.6.0
Release Date:
2021-10-05

CMS users without limited permissions to view data may be able access privileged information via the /admin/graphql endpoint because of a missing canView() on data. This affects data classes that utilise or inherit from the Read or ReadOne GraphQL 3 classes that don't explicitly assign a service class to the permissionChecker property of their implementation. On a default installation this will expose limited (ID, FirstName, Surname) information from the Member table which a CMS user typically will not have access to.

Graphql 4 is not affected by this.

If you have a legitimate use for an ItemQuery/ListQuery scaffolder class without a permission checker, you can use the following example.

```
# Put this in `app/_config/mysite.yml` on another config file
SilverStripe\Core\Injector\Injector:
  My\App\QueryPermissionChecker.nocheck:
    class: My\App\NoCheckPermissionChecker
  My\App\CustomItemQueryScaffolder:
    properties:
      permissionChecker: '%$My\App\QueryPermissionChecker.nocheck'
  My\App\CustomListQueryScaffolder:
    properties:
      permissionChecker: '%$My\App\QueryPermissionChecker.nocheck'
```

```
<?php

namespace My\App;

use SilverStripe\GraphQL\Permission\QueryPermissionChecker;
use SilverStripe\ORM\Filterable;
use SilverStripe\Security\Member;

class NoCheckPermissionChecker implements QueryPermissionChecker
{
    public function applyToList(Filterable $list, Member $member = null)
    {
        return $list;
    }

    public function checkItem($item, Member $member = null)
    {
        return true;
    }
}
```

Base CVSS: 3.0 (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:X/RL:O/RC:C&version=3.1)

CWP CVSS: 3.0 (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:X/RL:O/RC:C&version=3.1)

Reporters:

- ZX Security Ltd (https://zxsecurity.co.nz/)
- Luke Edwards (https://www.dna.co.nz/about/?staff=luke+edwards) from DNA Design (lukereative (https://github.com/lukereative) on GitHub)

OPEN SOURCE (/) COMPANY (HTTP://WWW.SILVERSTRIPE.COM) CLOUD PLATFORM (HTTPS://WWW.SILVERSTRIPE.COM/PLATFORM/)

(http://github.com/silverstripe) (http://vimeo.com/silverstripe) (http://facebook.com/silverstripe) (https://www.linkedin.com/company/silverstripe/) (http://twitter.com/silverstripe) Meetup (http://silverstripe.meetup.com/)

Privacy Policy (/home/footer-menu/privacy-policy/) Branding guidelines (https://www.silverstripe.com/about-us/our-brand/) BSD License (/software/bsd-license/)