CVE-2020-26136 GraphQL doesn't honour MFA when using basic auth

Severity:
Medium (? (https://docs.silverstripe.org/en/contributing/release_process/#security-releases))
Identifier:
CVE-2020-26136
Versions Affected:
silverstripe/graphql: ^3.0.0, ^4.0.0-alpha1
Versions Fixed:
silverstripe/graphql: ^3.5.0, ^4.0.0-alpha2
Release Date:
2021-06-08

The GraphQL module accepts basic-auth as an authentication method by default. This can be used to bypass MFA authentication if the silverstripe/mfa module is installed, which is now a commonly installed module. A users password is still required though.

Basic-auth has been removed as a default authentication method. It desired, it can be re-enabled by adding it to the authenticators key of a schema, or on SilverStripe\Graphql\Auth\Handler, i.e.

```
authenticators:
  -
    class: SilverStripe\GraphQL\Auth\BasicAuthAuthenticator
    priority: 20
```

Base CVSS: 4.2 (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N&version=3.1)

CWP CVSS: 4.2 (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N&version=3.1)

Reporters: Maxime Rainville from Silverstripe Ltd (https://www.silverstripe.com)
(https://zxsecurity.co.nz)

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

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