CVE-2020-26138 FormField with square brackets in field name skips validation

Severity:
Low (? (https://docs.silverstripe.org/en/contributing/release_process/#security-releases))
Identifier:
CVE-2020-26138
Versions Affected:
silverstripe/framework: ^3.0.0, ^4.0.0
Versions Fixed:
silverstripe/framework: ^4.7.4, ^4.8.0
Release Date:
2021-06-08

FileField with array notation skips validation

The FileField class is commonly used for file upload in custom code on a Silverstripe website. This field is designed to be used with a single file upload.

PHP allows for submitting multiple values by adding square brackets to the field name. When this is done to a FileField, it will be coerced into allowing multiple files by using this notation. This is not a supported feature, though nothing is done to prevent this.

In this scenario, validation such as limiting allowed extensions is not applied, and the FileField->saveInto() behaviour is not triggered. If custom controller logic is used to process the file uploads, it might implicitly rely on validation to be provided by the Form system, which is not the case.

Note this issue is for the FileField, not the UploadField which is used within the CMS.

Example:

```
public function MyForm()
{
  $fields = FieldList::create(
    FileField::create('MySafeField')->setAllowedExtensions(['pdf']),
    FileField::create('MyUnsafeField[]')->setAllowedExtensions(['pdf'])
  );
  $actions = FieldList::create(
    FormAction::create('submit')
  );
  $validator = RequiredFields::create('MySafeField', 'MyUnsafeField');
  return Form::create($this, 'Form', $fields, $actions, $validator);
}

public function submit($data, $form)
{
  $data['MyUnsafeField'] // not validated
  $_FILES['MyUnsafeField'] // not validated
}
```

Base CVSS: 3.4 (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C&version=3.1)

CWP CVSS: 3.4 (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C&version=3.1)

Reporters: Dylan Wagstaff from Silverstripe Ltd
(https://www.silverstripe.com)

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/)