Stored XSS in upload files

Low **PierreRambaud** published **GHSA-rc8c-v7rq-q392** on Sep 24, 2020

Package

No package listed

Affected versions

> 1.5.0.0

Patched versions

1.7.6.8

Description

Impact

Users are allowed to send compromised files, these attachments allowed people to input malicious JavaScript which triggered XSS payload

Patches

The problem is fixed in 1.7.6.8

Workarounds

With apache

In your `.htaccess` file

```
    <FilesMatch "\.pdf$">
      Header set Content-Disposition "Attachment"
      Header set X-Content-Type-Options "nosniff"
    </FilesMatch>
```

In your `/upload/.htaccess` file

```
  <IfModule mod_headers.c>
    Header set Content-Disposition "Attachment"
    Header set X-Content-Type-Options "nosniff"
  </IfModule>
```

With Nginx

```
  location ~* \.pdf$ {
    add_header Content-Disposition Attachment;
    add_header X-Content-Type-Options nosniff;
  }

  location ~ ^/upload/ {
    add_header Content-Disposition Attachment;
    add_header X-Content-Type-Options nosniff;
  }
```

References

Cross-site Scripting (XSS) - Stored (CWE-79)

Severity

Low

CVE ID

CVE-2020-15162

Weaknesses

No CWEs

Credits

mikakulmala