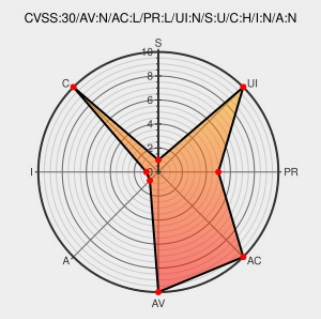
# CVE-2017-16790

Published on: 08/06/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:38 PM UTC

## CVE-2017-16790

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Debian Linux from Debian contain the following vulnerability:

An issue was discovered in Symfony before 2.7.38, 2.8.31, 3.2.14, 3.3.13, 3.4-BETA5, and 4.0-BETA5. When a form is submitted by the user, the request handler classes of the Form component merge POST data and uploaded files data into one array. This big array forms the data that are then bound to the form. At this stage there is no difference anymore between submitted POST data and uploaded files. A user can send a crafted HTTP request where the value of a "FileType" is sent as normal POST data that could be interpreted as a local file path on the server-side (for example, "file:///etc/passwd"). If the application did not perform any additional checks about the value submitted to the "FileType", the contents of the given file on the server could have been exposed to the attacker.

CVE-2017-16790 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

### CVSS3 Score: 6.5 - MEDIUM

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| NETWORK | LOW | LOW | NONE |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| UNCHANGED | HIGH | NONE | NONE |

### CVSS2 Score: 4 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | LOW | SINGLE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| PARTIAL | NONE | NONE |

## CVE References

| Description | Tags | Link |
|---|---|---|
| CVE-2017-16790: Ensure that submitted data are uploaded files (Symfony Blog) | Issue Tracking, Patch, Vendor Advisory, symfony.com, text/html | CONFIRM symfony.com/blog/cve-2017-16790-ensure-that-submitted-data-are-uploaded-files |
| Debian -- Security Information -- DSA-4262-1 symfony | Third Party Advisory, www.debian.org, Depreciated Link, text/html | DEBIAN DSA-4262 |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Application | Sensiolabs | Symfony | All | All | All | All |
| Application | Sensiolabs | Symfony | All | All | All | All |
| Application | Sensiolabs | Symfony | All | All | All | All |
| Application | Sensiolabs | Symfony | All | All | All | All |

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:a:sensiolabs:symfony:*:*:*:*:*:*:*:*:

cpe:2.3:a:sensiolabs:symfony:*:*:*:*:*:*:*:*:

cpe:2.3:a:sensiolabs:symfony:*:*:*:*:*:*:*:*:

cpe:2.3:a:sensiolabs:symfony:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

**CVE.report and Source URL Uptime Status status.cve.report**