Local File Inclusion

Affecting pimcore/pimcore package, versions **<6.8.8**

INTRODUCED: 18 FEB 2021 CVE-2021-23340 CWE-23 FIRST ADDED BY SNYK

Share

How to fix?

Upgrade `pimcore/pimcore` to version 6.8.8 or higher.

Overview

pimcore/pimcore is a content & product management framework (CMS/PIM/E-Commerce).

Affected versions of this package are vulnerable to Local File Inclusion. A Local FIle Inclusion vulnerability exists in the `downloadCsvAction` function of the `CustomReportController` class (`bundles/AdminBundle/Controller/Reports/CustomReportController.php`). An authenticated user can reach this function with a GET request at the following endpoint: `/admin/reports/custom-report/download-csv?exportFile=&#91;filename]` . Since `exportFile` variable is not sanitized, an attacker can exploit a local file inclusion vulnerability.

PoC

```
* Login in Pimcore * Send a GET request to the endpoint: /admin/reports/custom-report/download-csv?
exportFile=../../../../../../../../../../../../../../../etc/passwd to retrieve del passwd file of the Linux system. (Inside
the request insert the header X-pimcore-csrf-token).
```

References

- GitHub Additional Information
- GitHub Commit

Snyk CVSS

Exploit Maturity	Mature
Attack Complexity	Low
Confidentiality	HIGH

See more

NVD 7.1 HIGH

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.

Test your applications

Snyk Learn

Learn about Local File Inclusion vulnerabilities in an interactive lesson.

Start learning

Snyk ID	SNYK-PHP-PIMCOREPIMCORE-1070132
Published	18 Feb 2021
Disclosed	18 Feb 2021
Credit	Daniele Scanu

Report a new vulnerability | Found a mistake?