snyk Vulnerability DB

Snyk Vulnerability Database > Composer > pimcore/pimcore

Local File Inclusion

Affecting pimcore/pimcore package, versions <6.8.8



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=8#91; filename]. Since exportFile variable is not sanitized, an attacker can exploit a local file inclusion vulnerability.

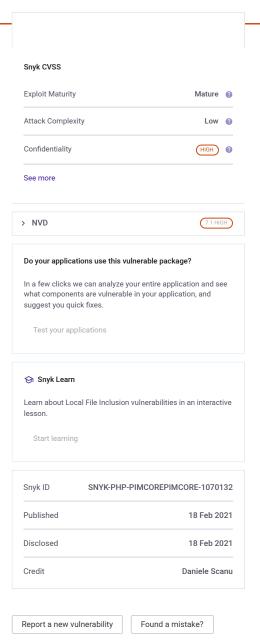
PoC

* 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



Q Search by package name or CVE

PRODUCT
Snyk Open Source
Snyk Code
Snyk Container
Snyk Infrastructure as Code
Test with Github
Test with CLI
RESOURCES
Vulnerability DB
Documentation

Blog FAQs

COMPANY

About

Jobs

. .

Policies

Do Not Sell My Personal Information

CONTACT US

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT





© 2022 Snyk Limited

Registered in England and Wales. Company number: 09677925

Registered address: Highlands House, Basingstoke Road, Spencers Wood, Reading, Berkshire, RG7 1NT.