

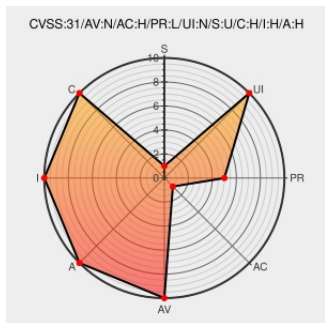


CVE-2022-31092

Published on: Not Yet Published

Last Modified on: 07/08/2022 06:49:00 PM UTC

CVE-2022-31092 - advisory for GHSA-gvmf-wcx6-p974

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Pimcore](#) from [Pimcore](#) contain the following vulnerability:

Pimcore is an Open Source Data & Experience Management Platform. Pimcore offers developers listing classes to make querying data easier. This listing classes also allow to order or group the results based on one or more columns which should be quoted by default. The actual issue is that quoting is not done properly in both cases, so there's the theoretical possibility to inject custom SQL if the developer is using this methods with input data and not doing proper input validation in advance and so relies on the auto-quoting being done by the listing classes. This issue has been resolved in version 10.4.4. Users are advised to upgrade or to apply the patch manually. There are no known workarounds for this issue.

CVE-2022-31092 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [pimcore](#) - **pimcore** version < 10.4.4

CVSS3 Score: **8.1 - HIGH**

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

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
[Security] SQL Injection in Data Hub GraphQL (#12444) · pimcore/pimcore@21559c6 · GitHub	github.com text/html	 MISC github.com/pimcore/pimcore/commit/21559c6bf0e4e828d33ff7af6e88caecb5ac6549
[Security] SQL Injection in Data Hub GraphQL by mcop1 · Pull Request #12444 · pimcore/pimcore · GitHub	github.com text/html	 MISC github.com/pimcore/pimcore/pull/12444
Improper quoting of columns when using setOrderBy() or setGroupBy() on listing classes · Advisory · pimcore/pimcore · GitHub	github.com text/html	 CONFIRM github.com/pimcore/pimcore/security/advisories/GHSA-gymf-wcx6-p974

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
Application	Pimcore	Pimcore	All	All	All	All
cpe:2.3:a:pimcore:pimcore:*****:.*.*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-31092 : Pimcore is an Open Source Data & Experience Management Platform. Pimcore offers developers listing... twitter.com/i/web/status/1...	2022-06-27 21:33:44
 /r/netcve	CVE-2022-31092	2022-06-27 22:39:05

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)