Improper quoting of columns when using setOrderBy() or setGroupBy() on listing classes

High **brusch** published **GHSA-gvmf-wcx6-p974** on Jun 22

Package

php **pimcore/pimcore** (Composer)

Affected versions	Patched versions
< 10.4.4	10.4.4

Description

Impact

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.

Example:

```
// request url: https://example.com/foo?groupBy=o_id`; SELECT SLEEP(20);--

$list = new DataObject\Car\Listing();
$list->setOrderKey($request->get('orderBy'));
$list->setGroupBy($request->get('groupBy'));
$list->load();
```

Patches

Upgrade to >= 10.4.4 or apply the following patch manually:
https://github.com/pimcore/pimcore/commit/21559c6bf0e4e828d33ff7af6e88caecb5ac6549.patch

Workarounds

Apply this patch manually:
https://github.com/pimcore/pimcore/commit/21559c6bf0e4e828d33ff7af6e88caecb5ac6549.patch

References

#12444

Severity

High

CVE ID

CVE-2022-31092

Weaknesses

CWE-89