# CVE-2022-31260

**Vendor:** Montala

**Product:** ResourceSpace

**Affected versions:** <= 9.8

ResourceSpace is web-based open source Digital Asset Management (DAM) software written in PHP.

## Incorrect Access Controls

A backdoor exists in legacy versions of "csv_export_results_metadata.php", which allows an unauthenticated user to export potentially sensitive collection metadata with a simple GET request ("k" parameter must not be null), e.g:

```
https://www.example.com/pages/csv_export_results_metadata.php?
k=zulu&personaldata=0&allavailable=true&submit=1
```

The metadata can contain personal data, and in fact the application has a commensurate feature which allows admins to redact such data from exports obtained via the usual mechanism.

The vendor has patched the vulnerability in the latest development release of version 9.8 (revision r19636).

Old file header:

```
<?php
include_once '../include/db.php';
# External access support (authenticate only if no key was provided)
if(getvalescaped('k', '') == '')
    {
    include_once '../include/authenticate.php';
    }
```

Revised file header:

```
<?php
include_once '../include/db.php';
include_once '../include/authenticate.php';
```