DBFile permission bypass

Moderate **emteknetnz** published **GHSA-jgcf-rf45-2f8v** 4 days ago

Package

php **silverstripe/assets** (Composer)

Affected versions	Patched versions
<2.4.5	2.4.5
>=3.0.0, <3.1.3	3.1.3

Description

Impact

Images rendered in templates or otherwise accessed via `DBFile::getURL()` or `DBFile::getSourceURL()` incorrectly add an access grant to the current session, which bypasses file permissions.

This usually happens when creating an image variant, for example using a manipulation method like `ScaleWidth()` or `Convert()`.

Note that if you use `DBFile` directly in the `$db` configuration for a `DataObject` class that doesn't subclass `File`, and if you were setting the visibility of those files to "protected", those files will now need an explicit access grant to be accessed. If you do not want to explicitly provide access grants for these files (i.e. you want these files to be accessible by default), you should use the "public" visibility.

Reported by

Restruct web & apps

References

- https://www.silverstripe.org/download/security-releases/cve-2026-24749

Severity

Moderate 5.3 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity	None
Availability	None

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVE ID

CVE-2026-24749

Weaknesses

No CWEs