Possible XSS attack via page revision comparison view

Moderate **gasman** published **GHSA-v2wc-pfq2-5cm6** on Apr 14, 2020

Package

wagtail (PyPI)

Affected versions

1.9 - 2.7.1, 2.8

Patched versions

2.7.2, 2.8.1

Description

Impact

A cross-site scripting (XSS) vulnerability exists on the page revision comparison view within the Wagtail admin interface. A user with a limited-permission editor account for the Wagtail admin could potentially craft a page revision history that, when viewed by a user with higher privileges, could perform actions with that user's credentials. The vulnerability is not exploitable by an ordinary site visitor without access to the Wagtail admin.

Patches

Patched versions have been released as Wagtail 2.7.2 (for the LTS 2.7 branch) and Wagtail 2.8.1 (for the current 2.8 branch).

Workarounds

Site owners who are unable to upgrade to the new versions can disable the revision comparison view by adding the following URL route to the top of their project's `urls.py` configuration:

```
from django.views.generic.base import RedirectView

urlpatterns = [
    url(r'^admin/pages/(\d+)/revisions/compare/', RedirectView.as_view(url='/admin/')),
    # ...
]
```

Acknowledgements

Many thanks to Vlad Gerasimenko for reporting this issue.

For more information

If you have any questions or comments about this advisory:

- Visit Wagtail's support channels
- Email us at security@wagtail.io (if you wish to send encrypted email, the public key ID is `0x6ba1e1a86e0f8ce8`)

Severity

Moderate

CVE ID

CVE-2020-11001

Weaknesses

No CWEs