Django security releases issued: 4.0.2, 3.2.12, and 2.2.27

Posted by **Mariusz Felisiak** on February 1, 2022

In accordance with our security release policy, the Django team is issuing Django 4.0.2, Django 3.2.12, and Django 2.2.27. These release addresses the security issues detailed below. We encourage all users of Django to upgrade as soon as possible.

CVE-2022-22818: Possible XSS via `{% debug %}` template tag

The **`{% debug %}`** template tag didn't properly encode the current context, posing an XSS attack vector.

In order to avoid this vulnerability, **`{% debug %}`** no longer outputs information when the **`DEBUG`** setting is **`False`**, and it ensures all context variables are correctly escaped when the **`DEBUG`** setting is **`True`**.

Thanks Keryn Knight for the report.

This issue has severity "medium" according to the Django security policy.

CVE-2022-23833: Denial-of-service possibility in file uploads

Passing certain inputs to multipart forms could result in an infinite loop when parsing files.

Thanks Alan Ryan for the report.

This issue has severity "medium" according to the Django security policy.

Affected supported versions

- Django main branch
- Django 4.0
- Django 3.2
- Django 2.2

Resolution

Patches to resolve the issue have been applied to Django's main branch and to the 4.0, 3.2, and 2.2 release branches. The patches may be obtained from the following changesets.

CVE-2022-22818:

- On the main branch
- On the 4.0 release branch
- On the 3.2 release branch
- On the 2.2 release branch

CVE-2022-23833:

- On the main branch
- On the 4.0 release branch
- On the 3.2 release branch
- On the 2.2 release branch

The following releases have been issued:

- Django 4.0.2 (download Django 4.0.2 | 4.0.2 checksums)
- Django 3.2.12 (download Django 3.2.12 | 3.2.12 checksums)
- Django 2.2.27 (download Django 2.2.27 | 2.2.27 checksums)

The PGP key ID used for this release is Mariusz Felisiak: 2EF56372BA48CD1B.

General notes regarding security reporting

As always, we ask that potential security issues be reported via private email to **`security@djangoproject.com`**, and not via Django's Trac instance or the django-developers list. Please see our security policies for further information.

Team Organization

Django Software Foundation

Code of Conduct

Diversity Statement

Get Involved

Join a Group

Contribute to Django

Submit a Bug

Report a Security Issue

Get Help

Getting Help FAQ

#django IRC channel

Django Discord

Official Django Forum

Follow Us

GitHub

Twitter

News RSS

Django Users Mailing List

Support Us

Sponsor Django

Official merchandise store

Amazon Smile

Benevity Workplace Giving Program