مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Multiple Vulnerabilities in Django Framework

Tracking #:432318350

Date:04-02-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed The Django Security Team has released urgent security updates addressing six vulnerabilities impacting supported Django versions.

TECHNICAL DETAILS:

The Django Security Team has released urgent security updates addressing six vulnerabilities impacting supported Django versions. These issues include three high-severity SQL injection flaws, two denial-of-service (DoS) vulnerabilities, and one username enumeration weakness.

Vulnerability Details:

- CVE-2026-1207 – High – SQL Injection via Raster Lookups on PostGIS Untrusted band index input in GIS raster lookups can lead to arbitrary SQL execution.
- CVE-2026-1287 – High – SQL Injection in Column Aliases via Control Characters FilteredRelation allows SQL injection through crafted column aliases using dictionary expansion.
- CVE-2026-1312 – High – SQL Injection via QuerySet.order_by() with FilteredRelation Column aliases containing periods can be exploited for SQL injection when combined with FilteredRelation.
- CVE-2025-14550 – Moderate – Denial of Service via Repeated Headers in ASGI Duplicate headers trigger super-linear string concatenation, enabling service degradation or outage.
- CVE-2026-1285 – Moderate – Denial of Service in HTML Truncator Parsing Large volumes of unmatched HTML end tags cause quadratic parsing time in Django truncation utilities.
- CVE-2025-13473 – Low – Username Enumeration via mod_wsgi Timing Attack Authentication timing differences allow remote attackers to enumerate valid usernames.

Affected Versions

- Django main branch
- Django 6.0 (prior to 6.0.2)
- Django 5.2 (prior to 5.2.11)
- Django 4.2 (prior to 4.2.28)

Fixed Versions:

- Django 6.0.2
- Django 5.2.11
- Django 4.2.28

RECOMMENDATIONS:

- Upgrade Django immediately to one of the fixed versions.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.djangoproject.com/weblog/2026/feb/03/security-releases/