مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates-Django Framework

Tracking #:432317962

Date:07-11-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that The Django development team has released security patches addressing two vulnerabilities — a SQL Injection flaw (CVE-2025-64459) and a Denial-of-Service (DoS) flaw (CVE-2025-64458).

TECHNICAL DETAILS:

The Django development team has released security patches for versions 5.2.8, 5.1.14, and 4.2.26, addressing two newly discovered vulnerabilities — a SQL Injection flaw (CVE-2025-64459) and a Denial-of-Service (DoS) flaw (CVE-2025-64458).

Vulnerability Details

1. CVE-2025-64459 — Potential SQL injection via _connector keyword argument in QuerySet and Q objects
   - CVSS 3.x:9.1 CRITICAL

2. CVE-2025-64458: Potential denial-of-service vulnerability in HttpResponseRedirect and HttpResponsePermanentRedirect on Windows
   - CVSS 3.x:7.5 HIGH

Updated Versions:

- Django 5.2.8, 5.1.14, and 4.2.26

RECOMMENDATIONS:

The UAE Cyber Security Council recommends administrators and developers must apply the patched versions immediately.

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/2025/nov/05/security-releases/