مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in Python

Tracking #:432317547

Date:29-07-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in Python that could potentially be exploited to cause denial-of-service (DoS) conditions on affected systems.

TECHNICAL DETAILS:

A security vulnerability in Python's standard tarfile module, tracked as **CVE-2025-8194**, may allow attackers to trigger **infinite loops and denial-of-service (DoS)** conditions by submitting specially crafted .tar archive files. This flaw affects **all Python versions prior to 3.14.0** and carries a **CVSS v4 base score of 7.5 (High)**.

Vulnerability Details:
The issue resides in the TarFile extraction and entry enumeration routines. When processing archive entries with negative offsets, the module fails to perform necessary validation, leading to an infinite loop during parsing.
Impact:

- Resource exhaustion
- Application hangs
- System unresponsiveness
- DoS attacks through untrusted .tar input

Affected Versions

- Python versions before 3.14.0

Fixed Version

- Python 3.14.0 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Python.

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://nvd.nist.gov/vuln/detail/CVE-2025-8194