مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Remote Code Execution (RCE) Vulnerability in python-json-logger

Tracking #:432316953

Date:10-03-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability (CVE-2025-27607) has been discovered in the widely used Python logging library, python-json-logger.

TECHNICAL DETAILS:

A critical vulnerability (CVE-2025-27607) has been discovered in the widely used Python logging library, **python-json-logger**. The vulnerability exposes systems to Remote Code Execution (RCE) via dependency hijacking, posing a significant risk to organizations using the library.

The issue stems from a missing optional dependency (msgspec-python313-pre) in versions 3.2.0 to 3.2.1, allowing attackers to inject malicious code by claiming the dependency on PyPI. This vulnerability is particularly exploitable in Python 3.13.x environments when installing the [dev] optional dependencies.

Key Details

- **CVE ID**:CVE-2025-27607
- **Vulnerability Type**: Remote Code Execution (RCE) via Dependency Hijacking
- **Affected Versions**: python-json-logger versions 3.2.0 to 3.2.1
- **Affected Environments**: Python 3.13.x with [dev] optional dependencies installed
- **CVSS v3 Score**: 8.8 (High)
- **Attack Vector**: Network
- **Exploit Availability**: Proof of Concept (PoC) available
- **Timeline**: Vulnerability existed from **December 30, 2024**, to **March 4, 2025**
- **Fixed Versions**: python-json-logger version 3.3.0 and later.

Potential Impact

- Remote Code Execution (RCE): Complete system compromise.
- Mass Exploitation Risk: Over 46 million downloads per month could result in widespread attacks.
- Supply Chain Attack Vector: Developers and enterprises relying on python-json-logger may be at risk.
- Data Breach & Malware Injection: Possible exfiltration of sensitive data.

RECOMMENDATIONS:

- Immediately update to python-json-logger 3.3.0 or later.
- Rebuild and redeploy impacted environments and applications to ensure malicious code is not present.
- Regularly audit third-party dependencies and ensure security patches are applied promptly.

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-2025-27607