مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in WhoDB Database Tool

Tracking #:432316847

Date:10-02-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities have been identified in the widely used database management tool WhoDB including a critical flaw.

TECHNICAL DETAILS:

Vulnerability Details

1. **CVE-2025-24786: Path Traversal Vulnerability (CVSS 10.0)**

- This critical vulnerability arises from improper path validation when opening SQLite3 databases in WhoDB. While the application is designed to limit access to SQLite3 databases within a specific directory, an attacker can exploit this flaw using path traversal techniques (e.g., ../../) in file paths. By navigating outside the intended directory, an attacker can access any SQLite3 database present on the host machine.

Impact:

- Unauthorized access to sensitive data stored in SQLite3 databases.
- Potential modification or corruption of critical information.
- Disruption of services relying on sensitive database files.

2. **CVE-2025-24787: Parameter Injection Vulnerability (CVSS 8.6)**

- This vulnerability stems from unsafe string concatenation when building database connection URIs in WhoDB. The flaw allows attackers to inject arbitrary parameters into the connection string, exploiting the allowAllFiles parameter in the github.com/go-sql-driver/mysql library. By injecting &allowAllFiles=true, attackers can execute the LOAD DATA LOCAL INFILE query, enabling them to read local files from the system running WhoDB.

Impact:

- Unauthorized access to local files on the host machine.
- Potential exposure of sensitive files, such as configuration files, credentials, or other private data.
- Increased risk of unauthorized system access and compromise.

Affected Versions:

- WhoDB versions <= 0.45.0

Fixed Versions:

- WhoDB versions >0.45.0

RECOMMENDATIONS:

- Users of WhoDB are strongly advised to update to the latest version as it addresses both vulnerabilities.
- Implement network segmentation to isolate WhoDB from other critical systems and reduce the potential attack surface.

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://github.com/clidey/whodb/security/advisories/GHSA-9r4c-jwx3-3j76
- https://github.com/clidey/whodb/security/advisories/GHSA-c7w4-9wv8-7x7c