مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in Exim Mail Server

Tracking #:432318188

Date:29-12-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed critical vulnerabilities in Exim mail server that could allow remote attackers to compromise affected systems under certain configurations. The issues stem from improper input handling and unsafe memory usage, potentially leading to unauthorized access or system instability.

TECHNICAL DETAILS:

Vulnerability Details

1) SQL Injection via Incomplete Escaping

- **CVE-2025-26794**
- CVSS Base Score: 9.8 (Critical)
- An incomplete fix in the xtextencode() function fails to properly escape single quote characters. This allows attackers to inject arbitrary SQL into SQLite hints database queries via crafted SMTP addresses.
- Successful exploitation may allow:
  - Execution of attacker-supplied SQL queries.
  - Retrieval of attacker-controlled binary data from the database.
  - Potential manipulation of internal Exim behavior.

2) Heap Buffer Overflow via bloom_size Manipulation

- The bloom_size parameter used for SQLite-based bloom filter operations is read directly from the database without validation.
  - The bloom filter array is allocated with a fixed size of 40 bytes.
  - An attacker can inject a database value causing bloom_size to be larger.
  - This results in memory writes far beyond allocated heap boundaries, leading to heap corruption.
- This condition can be triggered remotely through carefully crafted SMTP transactions when attacker-controlled data is used as a database key.

Affected Versions

- Exim 4.99

RECOMMENDATIONS:

- Review and update Exim Configurations.
- Apply available updates or patches when released
- Follow secure coding and deployment best practices to reduce exploitation risk

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://code.exim.org/exim/exim/src/commit/d46a6727798fc48d1756190a6d46d19216348c25/doc/doc-txt/exim-security-2025-12-09.1/report.txt