مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Critical Vulnerability in Exim MTA

Tracking #:432316053

Date:15-07-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Exim released security updates to address a critical vulnerability in Exim mail transfer agent (MTA).

TECHNICAL DETAILS:

Exim is a free mail transfer agent (MTA) that's widely used on Unix-like operating systems. A vulnerability in Exim MTA due to a bug in RFC 2231 header parsing could potentially allow remote attackers to deliver malicious attachments to user inboxes.

Exploit Availability: A Proof-of-concept (PoC) is available, but no active exploitation is known yet.

Vulnerability Details:

- **CVE-2024-39929** | CVSS 9.1– Critical
- The vulnerability could allow a remote attacker to bypass filename extension blocking protection measures and deliver executable attachments directly to end-users' mailboxes. If a user were to download or run one of these malicious files, the system could be compromised.

Affected versions:

- This vulnerability affects Exim releases up to and including 4.97.1

Fixed versions:

- This issue is fixed in Exim 4.98

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by Exim.

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-2024-39929