مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in Mozilla Thunderbird

Tracking #:432316512

Date:14-11-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in Mozilla Thunderbird that could be exploited to gain unauthorized access to sensitive information on affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-11159: Potential disclosure of plaintext in OpenPGP encrypted message**
- Severity- High
- The vulnerability stems from the way Thunderbird handles remote content in OpenPGP encrypted messages. When an encrypted message contains references to remote content, it can lead to the unintended disclosure of the message's plaintext.
- Successful exploitation of this vulnerability could result in Unauthorized access to the content of encrypted emails, Compromise of sensitive information intended to be protected by encryption, Potential breach of confidentiality for OpenPGP users.

Affected Versions:

- Thunderbird versions prior to 128.4.3
- Thunderbird versions prior to 132.0.1

Fixed Versions:

- Thunderbird 128.4.3
- Thunderbird 132.0.1

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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://www.mozilla.org/en-US/security/advisories/mfsa2024-61/
- https://www.mozilla.org/en-US/security/advisories/mfsa2024-62/