مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Hackers Exploiting Roundcube Webmail XSS Vulnerability

Tracking #:432316427

Date:23-10-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that threat actors are actively exploiting a now-patched cross-site scripting (XSS) vulnerability in Roundcube webmail software, which is being used in phishing attacks aimed at stealing user credentials.

TECHNICAL DETAILS:

Unknown threat actors have recently exploited a now-patched XSS vulnerability in the Roundcube webmail software, specifically CVE-2024-37383. This vulnerability has been leveraged in phishing attacks aimed at stealing user credentials.

Vulnerability Details:

- **CVE-2024-37383**
- **CVSS Score**: 6.1 (Medium Severity)
- The flaw allows attackers to execute arbitrary JavaScript by improperly processing SVG elements in emails, enabling credential theft when victims open malicious emails.

Attack Methodology:

1. **Phishing Email**: Attackers send emails that appear blank but contain hidden JavaScript payloads.
2. **Execution of Malicious Code**: The payload utilizes 'eval(atob(...))' to decode and execute JavaScript, which can manipulate the Roundcube interface.
3. **Credential Harvesting**:
    - A fake login form is displayed to capture user credentials.
    - Captured data is exfiltrated to a remote server (e.g., 'libcdn.org').

Affected Versions:

- Roundcube versions earlier than 1.5.6 and versions 1.6 to 1.6.6

Fixed Versions:

- Roundcube Versions 1.57, 1.67, 1.6.9 or later

Indicators of Compromise (IOCs):

- Presence of distinctive tags with eval(atob(...)) in email bodies
- Domain: libcdn.org (for sending stolen credentials)
- Domain: rcm.codes (for sending mailbox content)

MITRE ATT&CK Techniques:

- **Execution**: T059.007 (JavaScript)
- **Collection**: T1114.003 (Remote email collection), T1056.004 (Web portal capture)

RECOMMENDATIONS:

- **Update Immediately**: Upgrade Roundcube Webmail to the latest patched version
- **Email Filtering**: Implement strict email content filtering to block suspicious SVG elements and JavaScript

- **Network Monitoring**: Monitor for unexpected outbound connections, especially to the identified domains
- **User Awareness**: Educate users about the risks of interacting with unexpected email attachments or login prompts

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://global.ptsecurity.com/analytics/pt-esc-threat-intelligence/fake-attachment-roundcube-mail-server-attacks-exploit-cve-2024-37383-vulnerability