مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

RCE Vulnerability in Zimbra

Tracking #:432316354

Date:02-10-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed an actively exploited vulnerability discovered in Zimbra's postjournal service, that allows unauthenticated attackers to execute arbitrary commands on affected Zimbra installations.

TECHNICAL DETAILS:

Zimbra, a widely utilized email and collaboration platform, is facing a critical security vulnerability identified as CVE-2024-45519. This remote command injection flaw allows unauthenticated attackers to execute arbitrary commands on affected systems, potentially leading to full server control and significant data breaches. The vulnerability has been detected in mass exploitation campaigns, emphasizing the urgent need for immediate action from Zimbra administrators to mitigate risks.

CVE-2024-45519 is a remote command injection vulnerability located within Zimbra's postjournal service, which is responsible for processing SMTP messages. The flaw arises from improper handling of user input in the read_maps function, where user input is directly passed to the popen function without proper sanitization. This allows attackers to inject arbitrary shell commands.

Reports indicate that threat actors are actively exploiting CVE-2024-45519 using automated tools to target vulnerable Zimbra installations. Malicious emails have been traced back to specific IP addresses, highlighting ongoing exploitation attempts.

Fixed Versions:

- 9.0.0 Patch 41
- 10.0.9
- 10.1.1
- 8.8.15 Patch 46

RECOMMENDATIONS:

- Apply the latest security patches provided by Zimbra to address CVE-2024-45519. Ensure that all installations are updated to versions that mitigate this vulnerability.

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://wiki.zimbra.com/wiki/Zimbra_Security_Advisories