Nro. Alerta:	AL-2024-020	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR ALERTAS DE SEGURIDAD	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	16-oct-2024	VULNERABILIDAD EN EL SERVICIO POSTJOURNAL DE ZIMBRA	Pág.: **1** of **5**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad

Tipo de incidente: Información

Nivel de riesgo: Alto

II. ALERTA

Se ha identificado una vulnerabilidad crítica en Zimbra Collaboration Suite, específicamente en el servicio *Postjournal*. Esta vulnerabilidad permite la ejecución remota de comandos arbitrarios (RCE) por parte de atacantes no autenticados en versiones desactualizadas de Zimbra.

Figura 1.- *Ilustración asociada a ZIMBRA.* ***Fuente:*** *Cyber Security News*

III. INTRODUCCIÓN

La vulnerabilidad RCE se ha detectado en el servicio postjournal, que se utiliza para analizar los correos electrónicos entrantes a través de SMTP. Un atacante podría explotar la vulnerabilidad enviando correos electrónicos maliciosos con comandos para ejecutar en el campo CC, que luego se ejecutarían cuando el servicio postjournal procesa el correo electrónico.

Los investigadores de ProjectDiscovery han publicado un informe técnico (incluido en las referencias) que incluye una PoC. Además, se tiene constancia de la explotación activa de esta vulnerabilidad.

Se ha asignado el identificador CVE-2024-45519 para esta vulnerabilidad, que está disponible en el servicio de publicación de revistas en Zimbra Collaboration (ZCS) antes de 8.8.15 parche 46, 9 antes de 9.0.0 parche 41, 10 antes de 10.0.9 y 10.1 antes de 10.1.1 a veces permite a usuarios no autenticados ejecutar comandos.

IV. VECTOR DE ATAQUE:

Se ha descubierto que Zimbra usa el depósito S3 s3://repo.zimbra.com para alojar paquetes y parches. Afortunadamente, el depósito tenía una lista pública, lo que ha permitido localizar el parche necesario.

Para comenzar el análisis, se obtuvo la versión parcheada del binario posterior al diario del último paquete de parches de Zimbra: Zimbra Patch Package

Al extraer el archivo .deb, se recupera el binario del postjournal parcheado ubicado en ./opt/zimbra/lib/patches/postjournal.

En lugar de realizar una diferencia binaria, se opta por un enfoque más rápido invirtiendo el binario usando Ghidra. Se busca funciones críticas como system y exec* y se ha descubierto una función llamada run_command. read_maps, hizo referencia a esta función, lo que solicitó examinar read_maps y rastrear sus referencias hasta la función principal.

Establece la siguiente jerarquía de llamadas al método:

```
C

main
└── msg_handler(MSG *msg)
    └── expand_addrs
        └── address_lookup
            └── map_address
                └── read_addr_maps
                    └── read_maps
                        └── run_command
                            └── execvp
```

En la versión parcheada, se utiliza execvp y la entrada del usuario se pasa como una matriz, lo que evita la inyección directa de comandos. Además, notamos la introducción de una función is_safe_input que desinfecta la entrada antes de pasarla a execvp. Examinamos esta función para identificar cualquier carácter especial que pueda provocar la inyección de comandos.

```
int is_safe_input(char *input) {
    if (input == NULL || *input == '\0') {
        return 0;
    }
    for (char *c = input; *c != '\0'; c++) {
        if (*c == ';' || *c == '&' || *c == '|' || *c == '`' || *c == '$' ||
            *c == '(' || *c == ')' || *c == '<' || *c == '>' || *c == '\\' ||
            *c == '\'' || *c == '\"' || *c == '\n' || *c == '\r') {
            return 0;
        }
    }
    return 1;
}
```

NOTA: Más información en el siguiente link: **https://blog.projectdiscovery.io/zimbra-remote-code-execution/**

Del análisis de CVE-2024-45519 destaca una vulnerabilidad crítica en el servicio de publicación de diarios de Zimbra que permite la ejecución remota de comandos no autenticados. La vulnerabilidad se debe a que se pasan entradas no saneadas del usuario a popen en la versión sin parches, lo que permite a los atacantes inyectar comandos arbitrarios.

Si bien la versión parcheada introduce desinfección de entradas y reemplaza popen con execvp, mitigando la inyección directa de comandos, es crucial que los administradores apliquen los parches más recientes con prontitud. Además, comprender y configurar correctamente el parámetro mynetworks es esencial, ya que una configuración incorrecta podría exponer el servicio a una explotación externa.

V. IMPACTO:

Zimbra, una de las plataformas de colaboración y correo electrónico más utilizadas a nivel mundial, ha sido identificada recientemente como vulnerable a una falla de seguridad crítica que podría permitir a los atacantes tomar el control total de los sistemas afectados. La vulnerabilidad, rastreada como CVE-2024-45519, fue analizada por el investigador de seguridad Parth Malhotra de ProjectDiscovery, quien advierte de los graves riesgos que supone para las instalaciones de Zimbra. Al no requerir autenticación, esta vulnerabilidad ya ha sido detectada en campañas de explotación masiva. Se insta a los administradores de Zimbra a parchear sus sistemas de inmediato para evitar infracciones catastróficas.

CVE-2024-45519 es una vulnerabilidad de inyección remota de comandos en el servicio postdiario de Zimbra, un componente responsable de manejar mensajes SMTP. Esta vulnerabilidad permite a los atacantes ejecutar comandos arbitrarios en servidores vulnerables aprovechando el manejo inadecuado de la entrada del usuario. Fundamentalmente, no requiere autenticación, lo que significa que cualquiera con acceso a la red del servicio podría explotarlo. Una vez explotado, un atacante podría obtener control total sobre el servidor Zimbra, lo que provocaría el robo de datos, el compromiso del sistema y un posible movimiento lateral dentro de la red objetivo.

Una simple inyección provocó que el servidor ejecutara comandos arbitrarios, confirmando la existencia de la falla. El exploit inicial funcionó en el servicio postdiario que escuchaba en el puerto 10027, pero con los cambios de configuración adecuados, la vulnerabilidad también podría explotarse de forma remota a través de Internet.

ProjectDiscovery ha lanzado plantillas Nuclei que pueden detectar esta vulnerabilidad, que deben integrarse en los procesos de monitoreo de seguridad para identificar amenazas potenciales.

La gravedad de este defecto ha sido subrayada por informes de explotación masiva detectados en la naturaleza. Ivan Kwiatkowski, investigador principal de amenazas cibernéticas en HarfangLab, ha confirmado que los actores de amenazas están explotando activamente la vulnerabilidad CVE-2024-45519 en instalaciones vulnerables de Zimbra. Estos atacantes están utilizando herramientas automatizadas

para encontrar y explotar sistemas susceptibles, lo que añade urgencia a la necesidad de parches inmediatos.

VI. RECOMENDACIONES:

- Aplicar los parches más recientes de Zimbra, que reemplaza popen() por execvp() y utiliza una función de validación de entrada (is_safe_input()).
- Verificar la configuración de seguridad de Zimbra, asegurando que el servicio Postjournal no esté habilitado si no es necesario.
- Revisar el parámetro mynetworks en las configuraciones de Zimbra, ya que configuraciones incorrectas podrían permitir el acceso remoto no autorizado.
- No hacer clic en enlaces de fuentes no confiables.
- Tener cuidado con la información que se ingresa en formularios de sitios web.
- Implementar autenticación de dos factores para su cuenta.

VII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

VIII. REFERENCIAS:

- https://csirt.gob.cl/alertas/vsa24-01088/
- MISC:https://wiki.zimbra.com/wiki/Security_Center
- MISC:https://wiki.zimbra.com/wiki/Zimbra_Responsible_Disclosure_Policy
- https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories
- **https://blog.projectdiscovery.io/zimbra-remote-code-execution/**
- https://securityonline.info/poc-exploit-releases-for-zimbra-rce-flaw-cve-2024-45519-mass-exploitation-detected/