BOLETÍN DE ALERTA

Boletín Nro.: 2019-01
Fecha de publicación: 30/04/19.
Fecha de actualización: 31/05/19
Tema: Explotación masiva de vulnerabilidades en ZIMBRA

Sistemas afectados:

Zimbra Colaboration Suite (ZCS).

Descripción:

Recientemente se han reportado múltiples compromisos de servidores correo Zimbra, debido a la explotación masiva de las vulnerabilidades CVE-2016-9924, CVE-2018-20160, CVE 2019-9670 y CVE 2019-9621. Varios CSIRTs regionales han informado también sobre eventos de explotación masiva de estas vulnerabilidades.

Algunos de los indicios visibles que pueden indicar un compromiso del servidor Zimbra son los siguientes:

- Webmail en blanco después del login.
- Error al adjuntar ficheros, cuando antes no sucedía.
- "AJAX webmail not loading".

Se han identificado al menos dos variantes de explotación de estas vulnerabilidades. En una de ellas, los atacantes explotan la vulnerabilidad e inyecta una webshell para, a través de ella inyectar scripts o binarios maliciosos, por ej. para minar criptomonedas. En la otra variante, que ha sido reportada en nuestro país en los últimos días, los atacantes explotan la vulnerabilidad para crear múltiples usuarios en Zimbra con privilegios de administrador, con el objetivo de enviar spam desde el servidor.

Se insta a todos los administradores de sistemas a:

- Verificar las versiones de Zimbra Colaboration Suite (Ver versiones con parches disponibles más adelante en la nota) y software de base.
- Verificar la no existencia de los siguientes ficheros en sus servidores Zimbra:
  - zmcat
  - s.sh
  - l.sh
  - r.sh
  - cr.sh
  - tmp.txt
  - ynwD.jsp

  - ikDB.jsp
  - LU4e.jsp
  - PS1q.jsp
  - ikDB.js
- Los archivos JSP son webshells utilizadas para ejecutar comandos en el servidor de forma remota. Además éstos están acompañados por archivos .java y archivos .class alojados bajo el path /opt/zimbra/jetty/. Se pueden buscar los mismos con los siguientes comandos:
  - find /opt/zimbra/jetty/ -name "*.jsp" -mtime -30 -ls
  - find /opt/zimbra/jetty/ -name "*_jsp.java" -mtime -30 -ls
  - find /opt/zimbra/jetty/ -name "*.class" -mtime -30 -ls
- Los nombres utilizados en los archivos (identificados hasta ahora) son strings cortos y aleatorios. De las búsquedas antes mencionadas, se debe realizar un análisis de los resultados ya que las búsquedas arrojaran múltiples archivos legítimos.
- Verificar los siguientes archivos y directorios dónde se han detectado múltiples web shells:
  - /opt/zimbra/jetty/work/zimbra/org/apache/jsp/downloads/
  - /opt/zimbra/jetty/work/zimbra/org/apache/jsp/img/
  - /opt/zimbra/jetty/webapps/zimbra/downloads/
- Realizar búsquedas de procesos en ejecución que hagan uso de los scripts y ejecutables mencionados por medio del comando (ps faux).
- Verificar que el atacante no haya creado cuentas de correo, especialmente después del 28/03/2019 (especialmente en el grupo administrador).
- Verificar las tareas en el cron del usuario Zimbra

Impacto

Estas vulnerabilidades, podrían permitir que un atacante remoto ejecute código malicioso en servidores de correo Zimbra, inyectar WebShells o crear usuarios con permisos de administrador.

Solución:

- Realizar una copia de seguridad del servidor de correo.
- Asegurar que el software se encuentre actualizado. Se pueden encontrar los últimos parches es: https://wiki.zimbra.com/wiki/Zimbra_Releases
- Error del WebClient en blanco (AJAX Webmail not loading), se debe ejecutar lo siguiente como usuario root:

  cd /opt/zimbra/mailboxd
  find webapps -type d -exec chmod 0755 {} \;
  find webapps -type d -exec chmod 0644 {} \;

- Reiniciar los servicios de Zimbra.
  su - zimbra
  zmcontrol restart

- Error adjunto ficheros al WebClient, se debe ejecutar lo siguiente como usuario root:

  chmod 0775 /opt/zimbra/data/tmp/upload

Prevención:

En caso de que se verifique el compromiso de un sistema, se recomienda de manera URGENTE:

- Realizar un respaldo del servidor de correo.
- Instalar las actualizaciones tanto del Sistema Operativo base como del ZCS (Ver parches disponibles).
- Eliminar los archivos subidos por el atacante.
- Interrumpir los procesos identificados como parte del ataque (de momento se han identificado procesos con los comandos s.sh, l.sh y zmcat).
- Notificar al CERT-PY incluyendo en el reporte versiones del Sistema Operativo base y versión de ZCS utilizada.

Dado que no es posible validar la totalidad de las acciones realizadas por el atacante, se recomienda:

- Analizar la migración a un nuevo servidor en versión de Sistema Operativo y ZCS estable y con los últimos parches de seguridad instalados.
- Guardar una copia de la información de auditoría del Sistema Operativo base (/var/log) y de ZCS (/opt/zimbra/logs) para un eventual análisis.
- Analizar equipos aledaños para descartar movimientos laterales del atacante

Recomendaciones para limpiar zmcat

Ya que no podemos estar 100% seguros del daño que ha realizado zmcat al sistema, además de las cuentas que ha creado, modificado, accedido, ficheros añadidos. Se debe verificar algún script extraño que se está ejecutando, y que procesos tiene con él.

- Buscar procesos que estén haciendo uso de wget.
- Eliminaremos todo lo que tengamos en /tmp/ por ejemplo el zmcat, los .sh, etc.
- Eliminar cualquier .jsp, and .java files creados en las últimas semanas, ya que seguramente tengan un nombre raro y sean parte de este ataque.
- Eliminar un fichero llamado ZimbraApps.jsp ya que es parte del ataque:
- Cambiar las contraseñas del sistema, ya que el atacante pudo haber tenido acceso completo al sistema. por lo que seguimos los siguientes pasos:
  zmldappasswd <random>
  zmldappasswd -r <random>
  zmldappasswd -a <random>
  zmldappasswd -n <random>
  zmldappasswd -p <random>

  zmmypasswd <random>
  zmmypasswd --root <random>

- Cambiar las claves de SSH:

  su - zimbra
  zmsshkeygen
  zmupdateauthkeys

Información adicional:

https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/comunicacion/noticias/alerta-para-administradores-de-zimbra

https://lorenzo.mile.si/zimbra-cve-2019-9670-being-actively-exploited-how-to-clean-the-zmcat-infection/961/

https://www.jorgedelacruz.es/2019/05/28/zimbra-resolver-zmcat-problema-de-webmail-en-blanco-error-al-adjuntar-ficheros-ajax-webmail-not-loading-cve-2019-9670/