BOLETÍN DE ALERTA

Boletín Nro.: 2020-15
Fecha de publicación: 04/06/2020
Tema: Vulnerabilidad de bajo riesgo en Zimbra permitiría la ejecución remota de código

Sistemas afectados:

- Zimbra en versiones anteriores a la 8.8.15 Parche 10
- Zimbra en versiones 9.x anteriores a la 9.0.0 Parche 3

Descripción:

Recientemente Zimbra ha lanzado los parches de seguridad **10** y **3** para las versiones **8.8.15** y **9.0.0** respectivamente, los mismos abordan una vulnerabilidad identificada y catalogada como **CVE-2020-12846** de **riesgo bajo**.

El fallo se da en el archivo **/service/upload**, ubicado dentro del componente **"Webmail Subsystem"**, y es mediante la subida de imágenes o "**avatar**" en la sección de contactos de la bandeja de entrada para un contacto en específico, en donde un atacante podría subir otros tipos de **archivos ejecutables.** Si bien es visualizado un error de "**Corruption File**" luego de esto, el archivo se sube igualmente y queda almacenado localmente dentro del directorio **/opt/zimbra/data/tmp/upload/**.

Impacto:

Un atacante podría aprovechar este fallo, subir un **archivo ejecutable** (**exe, sh, bat, jar**, son algunos ejemplos), logrando así la **ejecución de código malicioso** si el archivo es interpretado y ejecutado por el servidor web.

Solución y prevención:

- Aplicar la actualización de seguridad **8.8.15 Parche 10** y **9.0.0 Parche 3**:
    - Para las versiones 8.8.8 y superiores, ejecute los siguientes comandos

como usuario **root** en la terminal:

- En el caso plataformas **Ubuntu**:

```
sudo apt-get update
sudo apt-get upgrade
su - zimbra
zmcontrol restart
```

- En el caso plataformas **RedHat**:

```
yum clean metadata
yum check-update
yum update
su - zimbra
zmcontrol restart
```

- Las versiones anteriores a 8.8.8, ya no cuentan con soporte de seguridad, por lo que es recomendable la actualización a la versión **8.8.15 o 9.0.0** de zimbra.

Antes de esto es importante tener algunos aspectos en consideración:

- *Realizar una copia de seguridad, ya que una vez aplicado el parche no es posible volver a la versión anterior, y*
- *Cambiar al usuario zimbra (usuario creado durante la instalación de zimbra) antes de hacer uso de los comandos ZCS CLI.*

Información adicional:

- https://blog.zimbra.com/2020/06/new-zimbra-patches-9-0-0-patch-3-and-8-8-15-patch-10/
- https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P3
- https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P10
- https://vuldb.com/?id.155996