BOLETÍN DE ALERTA

Boletín Nro.: 2022-35
Fecha de publicación: 12/08/2022
Tema: Vulnerabilidad RCE explotada masivamente en Zimbra.

La vulnerabilidad está presente en las versiones anteriores a:

- Zimbra Collaboration Kepler 9.0.0 Parche 24.1
- Zimbra Collaboration Joule 8.8.15 Parche 31.1

Descripción:

Se ha informado sobre una vulnerabilidad que afecta a Zimbra, que permitiría a un atacante remoto realizar ejecución remota de código (*RCE*) y que además existen reportes de que está siendo explotada masivamente.

La vulnerabilidad identificada como CVE-2022-27925 de severidad alta, con puntuación asignada de 7.2. Esta se debe a la falla en la función *mboximport* del servidor Zimbra, que recibe un archivo ZIP y extrae los archivos encontrados en él. Un atacante sin credenciales administrativas podría aprovechar esta vulnerabilidad para realizar ejecución remota de código (*RCE*).

Impacto:

La explotación exitosa de esta vulnerabilidad permitiría a un atacante sin credenciales administrativas realizar ejecución remota de código (*RCE*) en el sistema afectado.

Solución:

Recomendamos actualizar a la última versión disponible, proporcionada por Zimbra en el siguiente enlace:

- https://wiki.zimbra.com/wiki/Zimbra_Releases

Mitigación:

Adicionalmente, en caso de no haber aplicado los parches de 8.8.15P31 o 9.0.0P24, es recomendable seguir los siguientes pasos de mitigación:

- Buscar en los registros (logs) cualquier solicitud con códigos de estado basados en *40x* para el servlet */service/extension/backup/mboximport* vulnerable.

- Inspeccionar minuciosamente el directorio de usuarios de Zimbra (generalmente */opt/zimbra/*) para identificar posibles *webshells* y cualquier otra evidencia de explotación.
- Utilizar las reglas de Yara proporcionadas aquí para identificar webshells relacionados.
- Buscar solicitudes entrantes en su servidor a archivos *JSP* que coincidan con rutas que no figuran en los archivos *JSP* válidos 8.8.15 y 9.0.0 detallados aquí.

Nota: Zimbra proporcionó una guía para realizar estos pasos en el siguiente enlace:

- https://wiki.zimbra.com/wiki/Steps_To_Rebuild_ZCS_Server

Información adicional:

- https://www.volexity.com/blog/2022/08/10/mass-exploitation-of-unauthenticated-zimbra-rce-cve-2022-27925/
- https://nvd.nist.gov/vuln/detail/CVE-2022-27925
- https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P31.1
- https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P24.1
- https://wiki.zimbra.com/wiki/Steps_To_Rebuild_ZCS_Server
- https://github.com/volexity/threat-intel/blob/main/2022/2022-08-10%20Mass%20exploitation%20of%20(Un)authenticated%20Zimbra%20RCE%20CVE-2022-27925/yara.yar