BOLETÍN DE ALERTA

Boletín Nro.: 2022-08

Fecha de publicación: 04/02/2022

Fecha de actualización: 08/02/2022

Tema: Vulnerabilidad de Cross-Site Scripting (XSS) en Zimbra 8.8.15.

Software afectado:

- **Zimbra en sus versiones 8.8.15 P29 y P30**

Descripción:

Se ha descubierto una vulnerabilidad de seguridad Zero-Day en Zimbra, plataforma de correo electrónico de código abierto, que comienza con una serie de correos electrónicos de *phishing* dirigidos (*spear phishing*) e incluyen la explotación de la vulnerabilidad llamada *Cross-Site Scripting* (XSS).

Esta vulnerabilidad fue identificada por investigadores en una serie de campañas de *phishing* dirigido contra uno de sus clientes por parte de un actor malicioso que se identifica como *TEMP_Heretic* y posiblemente sea proveniente de China. El análisis de los correos electrónicos de estas campañas de *spear phishing* condujo a un descubrimiento, el atacante trataba de explotar una vulnerabilidad de *Cross-Site Scripting* (XSS) de día cero (*zero day*) en la plataforma de correo electrónico de Zimbra.

Los investigadores afirman que la explotación exitosa de esta vulnerabilidad permitiría a un atacante ejecutar *JavaScript* arbitrario en sesión activa de Zimbra del usuario. Ellos también observaron que los atacantes intentaban cargar *JavaScript* para robar datos y archivos adjuntos del correo de los usuarios afectados.

Por otra parte, esta vulnerabilidad aún no cuenta con un CVE asignado y tampoco cuenta con una mitigación oficial publicada.

Impacto:

Un atacante podría realizar ataques de *Cross-Site Scripting* (XSS) robando información confidencial de los sistemas afectados.

Mitigación:

No se cuenta con una solución oficial, sin embargo, los investigadores realizaron pruebas llegando a la conclusión de que la versión 9.0.0 en adelante de Zimbra no se encuentra vulnerable, además los investigadores recomiendan las siguientes medidas para bloquear los ataques que causa esta vulnerabilidad:

- Todos los indicadores de compromiso que puede encontrarlos aquí deben bloquearse en la puerta de enlace de correo o/y el nivel de red. Puede seguir el siguiente enlace para bloquear dominios a nivel Zimbra.
- El administrador del servidor Zimbra debe analizar los datos de referencia históricas en busca de referencias y accesos sospechosos. La ubicación predeterminada de estos registros se puede encontrar en /opt/zimbra/log/access*.log
- Se debería considerar actualizar a la versión 9.0.0, ya que actualmente no existe una versión segura de 8.8.15.

Por lo que recomendamos actualizar si es posible a dicha versión. Adicionalmente recomendamos no abrir ningún correo/enlace desconocido y aguardar a que Zimbra publique de manera oficial las mitigaciones correspondientes a esta vulnerabilidad.

Para una mayor información sobre esta vulnerabilidad puede visitar el siguiente enlace.

Solución:

Si desea actualizar su Zimbra la versión 9.0.0 puede seguir en el siguiente enlace donde encontrará una guía de cómo hacerlo:

- https://zimbra.github.io/zimbra-9/upgrade.html

Adicionalmente se encuentra disponible el Changelog e información adicional sobre la versión 9.0.0 de Zimbra en el siguiente enlace:

- https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0

Recientemente Zimbra ha publicado un *hotfix* para mitigar esta vulnerabilidad para la versión 8.8.15p30. El *hotfix* está disponible a todos los usuarios por medio del soporte de Zimbra, también se encuentra disponible a partir del 5 de febrero del 2022 a través del siguiente enlace:

- https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P30

Para más información sobre el *hotfix* puede seguir el siguiente enlace:

- https://blog.zimbra.com/2022/02/hotfix-available-5-feb-for-zero-day-exploit-vulnerability-in-zimbra-8-8-15/

Información adicional:

- https://www.bleepingcomputer.com/news/security/zimbra-zero-day-vulnerability-actively-exploited-to-steal-emails/
- https://www.securityweek.com/volexity-warns-active-exploitation-zimbra-zero-day
- https://www.volexity.com/blog/2022/02/03/operation-emailthief-active-exploitation-of-zero-day-xss-vulnerability-in-zimbra/