BOLETÍN DE ALERTA

Boletín Nro.: 2020-03

Fecha de publicación: 30/01/2020

Tema: Vulnerabilidades de XSS (Cross Site Scripting) en plataformas Zimbra.

Las vulnerabilidades poseen un nivel de criticidad medio y los identificadores asociados son: CVE-2019-15313, CVE-2019-12427, CVE-2019-11318, CVE-2019-8947, CVE-2015-2249.

Sistemas afectados:

Zimbra Collaboration “Network Edition” y “Open-Source Edition”:

- Zimbra Collaboration anterior a 8.8.15 Patch 1, tiene una vulnerabilidad XSS reflexivo, a través de la consola de Administración.
- Zimbra Collaboration anterior a 8.8.12 Patch 1, tiene XSS persistente.
- Zimbra Collaboration 8.7.x - 8.8.11P2, tiene XSS no persistente.
- Zimbra Collaboration anterior a 8.6.0 patch 5, tiene XSS.

Descripción:

Recientemente, se han publicado avisos de vulnerabilidades de seguridad confirmadas, que fueron corregidas para servidores Zimbra Collaboration.

Estás fallas existen en el cliente web y la consola de administración, y dan lugar a una vulnerabilidad conocida XSS (Cross Site Scripting) en este caso se presentan de dos tipos:

- Almacenado o permanente: La inyección de código maliciosa queda almacenada en el servidor.
- Reflexivo o Reflejado: La inyección de código viaja por los parámetros del mensaje HTTP, pero no queda almacenada del lado del servidor.

Hasta el momento de escribir este boletín Zimbra Collaboration no ha brindado detalles de sobre las URL ni parámetros afectados, y tampoco se ha informado ninguna técnica de explotación.

Impacto:

Estas vulnerabilidades podrían permitir a un atacante remoto ejecutar código malicioso en servidores de correo zimbra y robar información potencialmente confidencial, entre otros ataques.

Solución

- Se recomienda actualizar los servidores Zimbra Collaboration a la última versión del software disponible en el sitio web oficial de descargas: https://wiki.zimbra.com/wiki/Zimbra_Releases
- Las actualizaciones para las diferentes versiones de Zimbra afectadas que resuelven las vulnerabilidades descritas en este boletín son:
    - Zimbra Collaboration 8.8.15, la falla se encuentra subsanada desde el Patch 1 , ver como actualizar aquí.
    - Zimbra Collaboration superior a 8.8.12 Patch 1, ver como actualizar aquí.
    - Zimbra Collaboration superior a 8.8.11 P2, ver como actualizar aquí.
    - Zimbra Collaboration 8.6.0 patch 5, es importante destacar que esta versión de zimbra ya ha dejado de recibir soporte, por lo que se aconseja actualizar a una versión más reciente, descargar aquí.

Prevención:

Seguir las recomendaciones indicadas en la sección “Prevención” del boletin anterior: https://www.cert.gov.py/application/files/9615/5933/5512/BOL-CERT-PY-2019-01_-_Alerta_para_administradores_ZIMBRA_v2.0.pdf

Información adicional:

- https://wiki.zimbra.com/wiki/Zimbra_Releases
- https://www.zimbra.com/downloads/zimbra-collaboration-open-source/
- https://www.zimbra.com/downloads/zimbra-collaboration/
- https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P1
- https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.12/P1