BOLETÍN DE ALERTA

Boletín Nro.: 2023-32
Fecha de publicación: 14/07/2023
Fecha de actualización: 02/08/2023
Tema: Vulnerabilidad *XSS* en Zimbra Collaboration Suite Versión 8.8.15 - Actualización

Software afectado:

- Zimbra Collaboration (ZCS), versión 8.8.15.

Descripción:

Se ha reportado un aviso de seguridad sobre una vulnerabilidad *Zero Day* que afecta a Zimbra 8.8.15, que permitiría a un atacante robar información confidencial del usuario, ejecutar código malicioso y poner en peligro la integridad de los datos del sistema afectado.

La vulnerabilidad fue identificada como CVE-2023-38750, sin severidad y sin puntuación asignada aún. Esta vulnerabilidad *Zero Day* del tipo *Cross-site Scripting* (XSS) explotada activamente se debe a una falla de validación de datos de entradas del usuario en Zimbra Collaboration. Esto permitiría a un atacante no autenticado a través de peticiones *HTTP* especialmente diseñadas, obtener información confidencial del usuario o ejecutar códigos JavaScript maliciosos en el navegador de las víctimas que visiten el sitio web afectado.

Impacto:

La explotación exitosa de esta vulnerabilidad permitiría a un atacante no autenticado realizar ataques del tipo *Cross-site Scripting (XSS)* a través del sitio web afectado.

Solución:

Recomendamos actualizar a la última versión disponible provista por el fabricante en el siguiente enlace:

- https://wiki.zimbra.com/wiki/Security_Center#:~:text=for%20mitigation%20steps.-,ZCS%2010.0.2%20Released,-ZCS%2010.0.2%20was

Adicionalmente, en caso de no poder acceder a la actualización, se recomienda temporalmente aplicar la corrección manual en todos los nodos de buzón de correo siguiendo los siguientes pasos:

- Es necesario realizar una copia de seguridad del siguiente archivo: */opt/zimbra/jetty/webapps/zimbra/m/momoveto.*
- Se debe editar dicho archivo e ir a la línea número 40 para la actualización.
- Actualizar el valor del parámetro como se indica a continuación:

```
<input name="st" type="hidden" value="${fn:escapeXml(param.st)}"/>
```

- Antes de la actualización, la línea aparecía de la siguiente manera:

```
<input name="st" type="hidden" value="${param.st}"/>
```

- Después de la actualización, la línea debería aparecer como se muestra a continuación

```
<input name="st" type="hidden" value="${fn:escapeXml(param.st)}"/>
```

Nota: No es necesario reiniciar el servicio Zimbra luego de aplicar los pasos de mitigación.

Información adicional:

- https://www.incibe.es/incibe-cert/alerta-temprana/avisos/0day-cross-site-scripting-en-zimbra-collaboration-suite
- https://securityaffairs.com/148880/security/zimbra-fixed-2023-38750-zcs.html
- https://blog.zimbra.com/2023/07/security-update-for-zimbra-collaboration-suite-version-8-8-15/?hss_channel=tw-6561812
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38750
- https://www.bleepingcomputer.com/news/security/zimbra-patches-zero-day-vulnerability-exploited-in-xss-attacks/#google_vignette
- https://wiki.zimbra.com/wiki/Security_Center#:~:text=for%20mitigation%20steps.-,ZCS%2010.0.2%20Released,-ZCS%2010.0.2%20was