# BOLETÍN DE ALERTA

**Boletín Nro.**: 2022-40
**Fecha de publicación**: 07/10/2022
**Fecha de actualización**: 18/10/2022
**Tema**: Explotación masiva de vulnerabilidad *RCE 0-day* en Zimbra – Actualización.
**Actualizaciones:**

- **18/10/2022:** Se han lanzado parches de actualizaciones para corregir la vulnerabilidad de día cero.

**La vulnerabilidad está presente en los siguientes sistemas:**

Zimbra instalado sobre alguno de estos sistemas operativos:

- Red Hat Enterprise Linux 8.
- Rocky Linux 8.
- CentOS 8.
- CentOS7.

**Descripción:**

Se ha informado sobre una vulnerabilidad de día cero (*0-day*) que afecta a Zimbra, que permitiría a un atacante remoto realizar ejecución remota de código (*RCE*). Existen reportes de que la misma está siendo explotada masivamente. Actualmente para esta vulnerabilidad ya existe un *PoC* publicado en Internet.

La vulnerabilidad identificada como CVE-2022-41352 de severidad crítica, con puntuación asignada de 9.8. Esta se debe a la falla en el método de control *cpio* del servicio de antivirus *Amavis* utilizado por Zimbra. Esto permitiría a un atacante enviar un archivo especialmente diseñado para realizar ejecución remota de código (*RCE*) en el sistema afectado, así también la misma permitiría introducir webshells en carpetas públicas para obtener una línea de comandos remoto.

Ejemplo:
*<dominio_mail>/public/ZimletCore.jsp*

**Impacto:**

La explotación exitosa de esta vulnerabilidad permitiría a un atacante obtener acceso total al servidor.

**Solución:**

Recomendamos acceder a los parches correspondientes proporcionados recientemente por el equipo de Zimbra en los siguientes enlaces:

- Zimbra 8.8.15
- Zimbra 9.0.0

**Mitigación:**
Adicionalmente, la vulnerabilidad de día cero CVE-2022-41352, puede ser mitigada mediante la instalación del paquete "*pax*", siguiendo los siguientes pasos:

**CentOS 7 y derivados:**

```
yum install pax
```

**CentOS 8 y derivados:**

```
dnf install spax
```

**Reiniciar el servicio Zimbra:**

```
sudo su zimbra -
zmcontrol restart
```

En implementaciones de Zimbra para Ubuntu la utilidad *pax* ya se encuentra instalada por defecto, por lo cual no es explotable y no se requiere acción adicional.

Recomendamos analizar y verificar los servidores, por archivos *.jsp* sospechosos en las carpetas del sistema, de tal forma a validar si los mismos han sido comprometidos. Preste especial atención a las siguientes carpetas o rutas:

- /opt/zimbra/jetty/webapps/zimbra/public/

**NOTA**: Tenga en cuenta que las webshells también podrían haber sido introducidas en otras carpetas del sistema y tener otros nombres.

**Información adicional:**

- https://www.cert.gov.py/wp-content/uploads/2022/10/BOL-CERT-PY-2022-40-Explotacion-masiva-de-vulnerabilidad-RCE-0-day-en-Zimbra.pdf
- https://www.rapid7.com/blog/post/2022/10/06/exploitation-of-unpatched-zero-day-remote-code-execution-vulnerability-in-zimbra-collaboration-suite-cve-2022-41352/
- https://nvd.nist.gov/vuln/detail/CVE-2022-41352

- https://attackerkb.com/topics/1DDTvUNFzH/cve-2022-41352/rapid7-analysis?referrer=activityFeed
- https://wiki.zimbra.com/wiki/Steps_To_Rebuild_ZCS_Server
- https://thehackernews.com/2022/10/zimbra-releases-patch-for-actively.html
- https://blog.zimbra.com/2022/10/new-zimbra-patches-9-0-0-patch-27-8-8-15-patch-34/