BOLETÍN DE ALERTA

Boletín Nro.: 2022-39.
Fecha de publicación: 11/10/2022.
Tema: Explotación masiva de múltiples vulnerabilidades en servidores de correo.

- **Descripción:**

Recientemente se han reportado múltiples incidentes de seguridad que derivan en la fuga de información sensible, principalmente a través de la explotación de vulnerabilidades presentes en servidores de correo como Zimbra y Microsoft Exchange, siendo éstos software muy utilizados en la región, y particularmente en Paraguay. Este tipo de técnicas están siendo utilizada por grupos hacktivistas principalmente en la región de Latinoamérica que apuntan como objetivo organizaciones gubernamentales, policiales y militares como los casos que cobraron relevancia entre ellos el caso de SEDENA (MÉXICO) y Estado Mayor Conjunto (CHILE),

En todos estos incidentes, los atacantes aprovechan vulnerabilidades ya conocidas, en servidores que no han aplicado los parches correspondientes. En los últimos tiempos se han publicado múltiples vulnerabilidades críticas, con diversos tipos de consecuencias o impactos, que van desde *server-side request forgery* (*SSRF*), escalamiento de privilegios hasta ejecución remota de código (*RCE*).

Actualmente, las principales vulnerabilidades explotadas activamente son las siguientes:

Zimbra:

- CVE-2022-27924: Permite a un atacante no autenticado inyectar código arbitrario mediante comandos de *memcache* en la víctima, esta vulnerabilidad ya fue alertada en abril del 2022, tal como detallamos en el siguiente enlace.
- CVE-2022-27925: Se debe a la falla en la función *mboximport* que recibe un archivo ZIP y extrae los archivos encontrados en él. Un atacante sin credenciales administrativas podría aprovechar esta vulnerabilidad para realizar ejecución remota de código (*RCE*) en el sistema afectado, la cual fue alertada en abril del 2022, tal como detallamos en el siguiente enlace.
- CVE-2022-37042, 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, la cual fue alertada en agosto 2022, tal como se detalla en el siguiente enlace.

- CVE-2022-41352: Vulnerabilidad de ejecución remota (RCE) que afecta a la utilidad cpio utilizada por AMAVIS (Antivirus utilizado en Zimbra). Se debe tener en cuenta que esta vulnerabilidad no se corrige a través de un parche de Zimbra, en la instalación de la utilidad "pax" no se tiene evidencia de explotación con fines de hacktivismo, pero sí para otros fines por el momento, tal como detallamos en el siguiente enlace.

Microsoft Exchange:

- ProxyNotShell
  - CVE-2022-41082, Esta vulnerabilidad explotada de día cero (*0-day*) se debe a una falla en el componente *PowerShell Handler*. Esto permitiría a un atacante realizar ejecución remota de código (*RCE*), tal como detallamos en el siguiente enlace.

  - CVE-2022-41040, Esta vulnerabilidad de día cero (*0-day*) se debe a un error de control de acceso del servidor Exchange. Esto permitiría a un atacante remoto realizar ataques del tipo *server-side request forgery* (*SSRF*), tal como detallamos en el siguiente enlace.
- ProxyLogon, ProxyShell es un conjunto de tres vulnerabilidades de seguridad que aún siguen siendo explotadas activamente (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207, CVE-2021-26855, CVE-2021-27065) que afectan a Microsoft Exchange Server y que conjuntamente pueden ser utilizadas para lograr ejecutar código arbitrario remotamente sin autenticación, tal como detallamos en el siguiente enlace.

Tenga en cuenta que estas vulnerabilidades citadas han sido comprobadas como utilizadas por grupos hacktivistas, sin embargo, podrían no ser las únicas.

Impacto:

La explotación exitosa de estas vulnerabilidades permitirían a un atacante comprometer íntegramente el servidor de correo, obteniendo acceso a todas las cuentas del mismo. Así también, podría utilizar el servidor de correo comprometido y desde ahí, realizar otros tipos de ataques que permitan vulnerar y comprometer otros activos de la red interna de la Entidad.

Recomendaciones:

Atendiendo la criticidad de los servidores de correo que centralizan mucha información y proporcionan acceso a otros activos de la organización recomendamos:

- Implementar políticas y procedimientos de Gestión documental segura, que incluya mínimamente clasificación de la información, mecanismos comunicación segura (canales de comunicación cifrados, niveles de acceso, cifrado de contenido, etc).
- Desarrollar e implementar políticas y procedimientos para la gestión de actualizaciones de los servidores críticos, que minimicen al máximo el tiempo desde la publicación de la vulnerabilidad hasta su mitigación o corrección.
- Así también, analizar la posibilidad de implementar actualizaciones automáticas correspondientes a cada servidor, en aquellos escenarios que sea posible hacerlo, por los mecanismos del propio servidor o mediante herramientas de terceros.

En el caso particular de Zimbra, en ambientes Unix (CentOS/Ubuntu) por ejemplo, es posible implementar actualizaciones automáticas, siguiendo alguna de las siguientes estrategias:

- Opción 1: (Recomendado) Mediante las herramientas de actualización automáticas propias del sistema operativo
    a. CentOS/RHEL: mediante la utilidad *yum-cron*

    Para más información ver el siguiente enlace.

    b. Ubuntu/Debian: mediante *Install Unattended Upgrades*

- Ver guía oficial en el siguiente enlace.

    c. Centos 8 y derivados de RHEL mediante la utilidad *dnf-automatic,* para más información ver el siguiente enlace.

- Opción 2: mediante un script personalizado que actualice únicamente el servicio de Zimbra
    i. Crear un script personalizado que realice la actualización de los paquetes específicos de zimbra, según la distribución de Linux correspondiente, ejemplo *actualización_zimbra.sh.* Puede utilizar el siguiente código publicado por el CERT-PY en el siguiente enlace mismo está disponible para usarse en el sistema operativo CentOS7
        1. *https://github.com/CERT-PY/linux-scripts/blob/main/update-zimbrav1-CentOS7.sh*
    ii. Crear una tarea programada con *crontab* que ejecute el script *actualización_zimbra.sh* de forma iterativa de acuerdo a la periodicidad deseada.
        1. crontab –e
        2. Agregar los parámetros necesarios para que el script y programación de ejecución, por ejemplo, en la siguiente línea

del crontab programa que el script "update-zimbrav1-CentOS7.sh" se ejecute todos los días de la semana a partir de las 02:30 a.m.

a. 30 02 * * * root /root/folder/update-zimbra-centos7.sh > /dev/null 2>&1

Para obtener más información acerca de *crontab* seguir este enlace.

Tenga en cuenta que este *script* es solo un ejemplo, recuerde personalizar el código según su necesidad o entorno, si usted por algún motivo no puede utilizar las estrategias propuestas puede ver la guía de referencia de actualización manual de Zimbra, ver enlace para Zimbra 9.x, enlace para Zimbra rama 8.x.

En productos Microsoft Exchange, debe estar al pendiente de las actualizaciones, parches y mitigaciones de seguridad recomendados por el fabricante; no se cuentan con herramientas de actualización automática nativa de exchange on-premise ver el siguiente enlace.

Nota: Para clientes de Microsoft Exchange online, no se necesita realizar ninguna acción.

En caso de que tenga indicios o sospeche que su servidor de correo haya sido comprometido, ya sea mediante la explotación de estas vulnerabilidades u otras, puede reportar el incidente a abuse@cert.gov.py.

Información adicional:

- https://www.cert.gov.py/wp-content/uploads/2022/10/BOL-CERT-PY-2022-38-Vulnerabilidades-de-dia-cero-en-Microsoft-Exchange-Server.pdf
- https://twitter.com/hiramcoop/status/1576614441453780994?t=-1s59A5Y-jXKFgnBaLOu9Q&s=08
- https://www.microsoft.com/security/blog/2022/09/30/analyzing-attacks-using-the-exchange-vulnerabilities-cve-2022-41040-and-cve-2022-41082/
- https://www.gteltsc.vn/blog/warning-new-attack-campaign-utilized-a-new-0day-rce-vulnerability-on-microsoft-exchange-server-12715.html
- https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/
- https://twitter.com/Cronup_CyberSec/status/1575601009753145344
- https://www.cronup.com/alerta-de-seguridad-nueva-vulnerabilidad-critica-para-microsoft-exchange-en-explotacion-activa-0-day-rce/
- https://nvd.nist.gov/vuln/detail/CVE-2022-37042
- https://nvd.nist.gov/vuln/detail/CVE-2022-41082
- https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P31