AGOSTO 2022

Error de omisión de autenticación en Zimbra permite a atacantes cargar archivos arbitrarios para realizar ejecución remota de código

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile (CSIRT de Gobierno) advierte a la comunidad del Estado y al público en general que en las últimas horas fue detectado un masivo error de omisión de autentificación que se está explotando activamente para comprometer los servicios de correo electrónico del servicio Zimbra Collaboration Suite (ZCS).

Problema

Zimbra Collaboration (ZCS) contiene una falla en la funcionalidad de importación de mbox, lo que permite que un atacante autenticado cargue archivos arbitrarios para realizar la ejecución remota de código (RCE). Esta vulnerabilidad se encadenó con el CVE-2022-37042, que permite la ejecución remota de código sin autenticar.

Implicancias

En general, los atacantes que están explotando esta vulnerabilidad implementan una serie de webshells para obtener acceso persistente a los servidores ZCS los que crean un nuevo archivo en el servidor que no existía previamente y una nueva URL a la que el atacante puede acceder para interactuar con el webshell.

En el servidor ZCS, si se realiza una solicitud a una URL que no existe, se obtendrá como respuesta "404 No encontrado". Sin embargo, una vez que se coloca un webshell, el comportamiento al acceder a un URI determinada cambia según la lógica presente en el webshell. A menudo, estas webshells no tienen lógica para manejar el caso en el que se realizan solicitudes que no están de acuerdo con la lógica del diseño del webshell y, en consecuencia, responderán con un código de estado "200 OK" con una respuesta de 0 bytes.

Una explotación exitosa permitiría a los atacantes implementar shells web en ubicaciones específicas en los servidores comprometidos para obtener acceso persistente.

Los análisis recientes de esta vulnerabilidad en la naturaleza han demostrado que existen más de 1.000 instancias de ZCS comprometidas por terceros alrededor del mundo que están utilizando los mismos nombres de webshell.

¿Cómo responder?

En caso de que su organización esté ejecutando una versión de Zimbra anterior al parche 33 de Zimbra 8.8.15 o al parche 26 de Zimbra 9.0.0, se recomienda actualizar de manera urgente al parche más reciente.

El CSIRT de gobierno también recomienda a las organizaciones que cuentan con Zimbra realizar un análisis completo del servidor y ejecutar siguientes acciones:

- Realizar una adquisición de memoria inicial para preservar cualquier rastro residente en la memoria de la actividad de un potencial atacante.

- Buscar en los registros cualquier solicitud con códigos de estado basados en 40x para el servlet vulnerable /service/extension/backup/mboximport.
- Inspeccionar minuciosamente el directorio de usuarios de Zimbra (generalmente /opt/zimbra/) para identificar posibles webshells y cualquier otra evidencia de explotación.
- Utilizar reglas de YARA[1] para identificar webshells relacionados.
- Buscar solicitudes entrantes a su servidor ZCS para archivos JSP que coincidan con rutas que no figuran en los archivos JSP válidos 8.8.15 y 9.0.0 correspondientes.
- NO OLVIDAR revisar los servidores adyacentes a su red ZIMBRA, pues si el servidor fue comprometido es altamente probable que el actor malicioso haya intentado realizar movimientos laterales para acceder a otros niveles de la institución. Tenga presente las diferentes fases de un ataque (CyberKillChain[2]).

Mitigaciones y parches ofrecidas por el fabricante

https://wiki.zimbra.com/index.php/Zimbra_Releases/8.8.15/P33

https://wiki.zimbra.com/index.php/Zimbra_Releases/9.0.0/P26

https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P24

https://blog.zimbra.com/2022/08/authentication-bypass-in-mailboximportservlet-vulnerability/

https://nvd.nist.gov/vuln/detail/CVE-2022-27925

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.08.12 12:02:32 -04'00'

[1] https://github.com/volexity/threat-intel/blob/main/2022/2022-08-10%20Mass%20exploitation%20of%20(Un)authenticated%20Zimbra%20RCE%20CVE-2022-27925/yara.yar
[2] https://www.netskope.com/es/security-defined/cyber-security-kill-chain