Nro. Alerta:	EC-2022-83	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	16-agosto-2022	**Error de omisión en Zimbra Collaboration Suite (ZCS)**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de incidente: Sistemas y/o software Abierto
Nivel de riesgo: Alto

II. INTRODUCCIÓN

Investigaciones dieron a conocer un error de omisión de autentificación que se está explotando activamente para comprometer los servicios de correo electrónico del servicio ZCS.

Figura 1. Ilustración asociada a Zimbra.
Fuente: Zimbra

III. ALERTA:

Zimbra es un groupware[1] que permite compartir, almacenar y organizar mensajes de correo electrónico, citas, contactos, tareas y documentos. Esta plataforma es utilizada por más de 200 000 empresas de más de 140 países, incluidas más de 1000 organizaciones gubernamentales y financieras.

En este sentido, investigadores de la firma de inteligencia de amenazas Veloxity; encontraron que 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).

El grupo de investigación descubrió evidencia que indica que la causa probable de estas infracciones fue la explotación de CVE-2022-27925, una vulnerabilidad de ejecución remota de código (RCE) en ZCS.

Los ciberdelincuentes implementaron una serie de webshells para obtener acceso persistente a los servidores ZCS; cada uno de estos webshells creó un nuevo archivo en el servidor que

[1] Servidor de mensajería de colaboración

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-83	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	16-agosto-2022	**Error de omisión en Zimbra Collaboration Suite (ZCS)**	V 1.1

no existía previamente y una nueva URL a la que el atacante podía acceder para interactuar con el webshell. Cabe señalar que las webshells implementadas no son novedosas y se encuentran disponibles en repositorios.

IV. VECTOR DE ATAQUE:

Sistema y/o Software Abierto

V. IMPACTO:

Una explotación exitosa permitiría a los atacantes implementar shells web en ubicaciones específicas en los servidores comprometidos para obtener acceso persistente; afectando a la Integridad, Confidencialidad y Disponibilidad.

VI. RECOMENDACIONES:

El EcuCert recomienda a su comunidad objetivo:

- En el caso de que su institución emplee una versión de Zimbra 8.8.15 parche 33 (8.8.15P33) o al parche 26 de Zimbra 9.0.0 (9.0.0P26); se recomienda actualizar a la versión más reciente.
- Revisar el directorio (/opt/zimbra/) y descartar la presencia de posibles webshells.
- Utilizar reglas de YARA y comparar la lista de archivos JSP de forma predeterminada para verificar la presencia de webshells (https://github.com/volexity/threat-intel/tree/main/2022/2022-08-10%20Mass%20exploitation%20of%20(Un)authenticated%20Zimbra%20RCE%20CVE-2022-27925).
- Revisar la infraestructura adyacente a los servidores de correo Zimbra a fin de descartar posibles movimientos laterales.
- Capacitar a todos los usuarios, mediante la concientización y simulaciones para reconocer e informar sobre intentos de phishing e ingeniería social.
- Implementar un plan de respuesta a emergencias de la Organización/Institución.
- En el caso de sufrir un ataque de proporciones mayores, contacte a las Autoridades competentes en base a la Normativa Legal Vigente a nivel Nacional.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-83	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	16-agosto-2022	**Error de omisión en Zimbra Collaboration Suite (ZCS)**	V 1.1

VII. Descargo de responsabilidad

- La información en la presente alerta; se proporciona "tal cual" solo con fines informativos. EcuCERT no respalda ningún producto o servicio comercial, incluidos los sujetos de análisis.
- Cualquier referencia a productos, procesos o servicios comerciales específicos por marca de servicio, marca comercial, fabricante o de otro modo, no constituye ni implica respaldo, recomendación o favorecimiento por parte del EcuCERT.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

VIII. Bibliografía.

Gatlán, S. (11 de 08 de 2022). *BleepingComputer*. Obtenido de BleepingComputer: https://www.bleepingcomputer.com/news/security/zimbra-auth-bypass-bug-exploited-to-breach-over-1-000-servers/

NVD. (03 de 05 de 2022). *NVD NIST*. Obtenido de NVD NIST: https://nvd.nist.gov/vuln/detail/CVE-2022-27925

Research, V. T. (10 de 08 de 2022). *Volexity*. Obtenido de https://www.volexity.com/blog/2022/08/10/mass-exploitation-of-unauthenticated-zimbra-rce-cve-2022-27925/

Zimbra. (s.f.). Obtenido de https://www.zimbra.com/

Zimbra. (10 de 08 de 2022). *Blog Zimbra*. Obtenido de Blog Zimbra: https://blog.zimbra.com/2022/08/authentication-bypass-in-mailboximportservlet-vulnerability/