Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

Zimbra lanza parche para vulnerabilidad de explotación activa en su suite de colaboración.

18/Octubre/2022

Contenido

Introducción 3
Zimbra corrige Vulnerabilidades 4
Resumen 4
Recomendaciones 6
Actualizaciones 6
Noticia Completa 7
Contactos de soporte 8

INTRODUCCIÓN

Zimbra ha lanzado parches para contener una falla de seguridad explotada activamente en su suite de colaboración empresarial que podría aprovecharse para cargar archivos arbitrarios en instancias vulnerables.

ZIMBRA CORRIGE VULNERABILIDADES

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2022_10_18_01
Clasificación de alerta:	Noticia
Tipo de Impacto:	Medio
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	10/18/2022
Es día cero (0 day):	No

RESUMEN

Registrado como CVE-2022-41352 (puntuación CVSS: 9,8), el problema afecta a un componente de la suite Zimbra llamado Amavis , un filtro de contenido de código abierto y, más específicamente, a la utilidad cpio que utiliza para escanear y extraer archivos.

A su vez, se dice que la falla tiene sus raíces en otra vulnerabilidad subyacente (CVE-2015-1197) que se reveló por primera vez a principios de 2015, que según Flashpoint se rectificó, solo para revertirse posteriormente en distribuciones de Linux posteriores.

"Un atacante puede usar el paquete cpio para obtener acceso a cualquier otra cuenta de usuario", dijo Zimbra en un aviso publicado la semana pasada, y agregó que "recomienda pax sobre cpio".

Las correcciones están disponibles en las siguientes versiones:

Zimbra 9.0.0 Parche 27
Zimbra 8.8.15 Parche 34

Todo lo que un adversario debe hacer para convertir la deficiencia en un arma es enviar un correo electrónico con un archivo adjunto TAR especialmente diseñado que, una vez recibido, se envía a Amavis, que utiliza el módulo cpio para desencadenar el exploit.

La compañía de ciberseguridad Kaspersky ha revelado que grupos APT desconocidos se han estado aprovechando activamente de la falla en la naturaleza, con uno de los actores "infectando sistemáticamente todos los servidores vulnerables en Asia Central".

Los ataques, que se desarrollaron en dos oleadas de ataques a principios y finales de septiembre, se dirigieron principalmente a entidades gubernamentales de la región, abusando del punto de apoyo inicial para lanzar shells web en los servidores comprometidos para actividades de seguimiento.

Según la información compartida por la empresa de respuesta a incidentes Volexity, se estima que aproximadamente 1600 servidores Zimbra se infectaron en lo que llama una "mezcla de ataques dirigidos y oportunistas".

"Algunas rutas web shell [...] se usaron en la explotación dirigida (probablemente APT) de organizaciones clave en el gobierno, las telecomunicaciones y TI, predominantemente en Asia; otras se usaron en la explotación masiva en todo el mundo", dijo la compañía en una serie de tuits

RECOMENDACIONES

- Los servidores expuestos externamente deben mantenerse al día con los parches y actualizaciones.

- Si se detecta malware en la red interna, debe mitigarse a la brevedad y de ser posible identificar su vector de ataque para corregir todo riesgo de frente a una futura infección.

- Se recomienda que habiliten la opción de detección "Software Potencialmente Dañino" para detectar archivos clasificados como Hacking Tool.

- Valide que los CVE mostrados en la tabla anterior ya fueron parchados por el área de IT.

ACTUALIZACIONES

- Zimbra 9.0.0 Parche 27

- Zimbra 8.8.15 Parche 34

Noticia Completa

https://devel.group/blog/zimbra-parcha-vulnerabilidad-de-explotacion/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757
El Salvador: +(503) 2249 4252
Honduras: +(504) 2283 5904
República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente