Observatorio de Derechos Digitales

Nueva vulnerabilidad encontrada en software comúnmente utilizado por el gobierno de Ecuador

Alerta No. 3
Noviembre 2023

¿Qué es lo nuevo? Google publicó hoy información sobre una vulnerabilidad de «día cero» recién descubierta encontrada en Zimbra, un paquete de código abierto para servidores de correo electrónico y trabajo colaborativo.

¿Por qué es importante? El gobierno de Ecuador corre varios servidores Zimbra y muchos de ellos no se han actualizado desde hace años. Eso significa que el sector público de Ecuador está especialmente vulnerable a ataques utilizando esta nueva vulnerabilidad.

¿Qué debe hacerse? Cualquier persona responsable de un servidor Zimbra necesita actualizarlo urgentemente a la última versión. Si eso no es posible, una medida temporal es prevenir ataques mediante el uso de firewalls y varios tipos de sistemas de detección de intrusiones. Los firewalls (cortafuegos) de aplicaciones, de estar disponibles, también pueden resultar útiles.

En junio de 2023, Google descubrió una nueva vulnerabilidad que se utilizaba para atacar a organizaciones que ejecutaban Zimbra. Esta vulnerabilidad era lo que se conoce como “día cero”, algo que los desarrolladores del software desconocían, lo que significa que no tenían días para solucionar el problema.

La vulnerabilidad es grave y podría usarse para robar tanto el contenido de correo electrónico, así como también credenciales utilizadas para acceder a cuentas de correo electrónico.

Desde entonces, Google ha observado cuatro campañas diferentes que utilizan esta vulnerabilidad de diversas formas. Aunque el problema se solucionó el 5 de julio de 2023, se produjeron varios ataques después de esta fecha, lo que indica que los servidores vulnerables continúan existiendo en el medio.

Los objetivos conocidos incluyen los gobiernos de Grecia, Moldavia, Túnez, Vietnam y Pakistán. Quienquiera que esté utilizando este ataque, parece tener preferencia por atacar al sector público de varios países.

El gobierno de Ecuador ha utilizado Zimbra tanto para correo electrónico como para trabajo colaborativo durante mucho tiempo. Existe un gran número de instancias de Zimbra en el país: una simple búsqueda muestra más de 1000 servidores conocidos, y el número real probablemente sea mucho más alto. Cada uno de ellos es vulnerable a ataques, si no ha sido actualizado durante los últimos meses.

Usando información pública se encontró al menos un servidor Zimbra gubernamental que no había sido actualizado desde 2014, y si tomamos en cuenta esto como indicativo del resto de la infraestructura, el sector público ecuatoriano está en grave riesgo.

Usando información pública se encontró al menos un servidor Zimbra gubernamental que no había sido actualizado desde 2014, y si tomamos en cuenta esto como indicativo del resto de la infraestructura, el sector público ecuatoriano está en grave riesgo.

La contramedida en este caso es simple, pero urgente y crucial. Todos los servidores deben estar actualizados a la última versión lanzada. También es

una buena idea que los ingenieros de infraestructura agreguen reglas a los sistemas de detección de intrusiones y firewalls para identificar posibles intentos de explotar este problema.

Finalmente, la vía más probable para la intrusión que utiliza esta vulnerabilidad se realiza a través de varios tipos de phishing, que engañan al usuario para que presione un enlace malicioso.

Por este motivo, nuestra recomendación habitual de tener mucho cuidado con los enlaces que llegan de fuentes no confiables es aún más crucial en este contexto. Simplemente no hagan clic en enlaces en correos electrónicos o mensajes

.

Con el apoyo de:

Centro de Autonomía Digital

Orden Conflicto Violencia
Programa de Investigación