BOLETÍN DE ALERTA

Boletín Nro.: 2023-39
Fecha de publicación: 25/08/2023
Tema: Vulnerabilidad de acceso no autorizado en Zimbra Collaboration Suite

Software afectado:

- Zimbra Collaboration Suite versiones 10.x anteriores a Daffodil 10.0.3
- Zimbra Collaboration Suite versiones 9.x anteriores a 9.0.0 Kepler Patch 35
- Zimbra Collaboration Suite versiones 8.x anteriores a 8.8.15 Joule Patch 42

Descripción:

Se ha reportado un nuevo aviso de seguridad sobre una vulnerabilidad de un solo clic "*one-click*" que afecta a Zimbra Collaboration Suite, que permitiría a un atacante no autenticado obtener acceso a una cuenta del sistema afectado.

La vulnerabilidad identificada como CVE-2023-41106, sin severidad ni puntuación asignada aún. Esta vulnerabilidad de un solo clic "*one-click*" se debe a una falla de seguridad en Zimbra Collaboration Suite. Esto permitiría a un actor malicioso no autenticado a través del envió de un enlace malicioso especialmente diseñado a la víctima, engañar a la misma para que haga clic en el enlace y proporcione sus credenciales de acceso a su cuenta de Zimbra.

Impacto:

La explotación exitosa de esta vulnerabilidad podría permitir a un actor malicioso obtener acceso no autorizado a cuentas del sistema afectado.

Solución:

Recomendamos instalar las actualizaciones correspondientes a cada versión provistas por el fabricante a través de los siguientes enlaces:

- Zimbra Collaboration Suite versión Daffodil 10.0.3.
- Zimbra Collaboration Suite versión 9.0.0 Kepler Patch 35.
- Zimbra Collaboration Suite versión 8.8.15 Joule Patch 42.

Adicionalmente, si no es posible aplicar las actualizaciones de forma inmediata, recomendamos seguir los siguientes pasos de mitigación:

- Habilitar la autenticación de dos factores para la cuenta de Zimbra.
- No realizar clic en ningún enlace de fuentes que no sean de confianza.
- Tener cuidado con la información que se ingresa en los formularios de los sitios web.

Información adicional:

- https://securityonline.info/cve-2023-41106-zimbra-collaboration-suite-vulnerability-could-allow-unauthenticated-access/#google_vignette
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41106
- https://blog.zimbra.com/2023/08/zimbra-security-update/
- https://wiki.zimbra.com/wiki/Zimbra_Two-factor_authentication
- Zimbra Releases/10.0.3 - Zimbra :: Tech Center
- Zimbra Releases/8.8.15/P42 - Zimbra :: Tech Center
- Zimbra Releases/9.0.0/P35 - Zimbra :: Tech Center