Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

Ataque logra robar código fuente al aplicativo LastPass.

26/Agosto/2022

Contenido

Introducción

Uno de los administradores de contraseñas más grandes del mundo con 25 millones de usuarios, LastPass, ha confirmado que ha sido pirateado . En un aviso publicado el 25 de agosto, Karim Toubba, CEO de LastPass, dijo que una parte no autorizada había robado "partes del código fuente y alguna información técnica patentada de LastPass".

LastPass

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

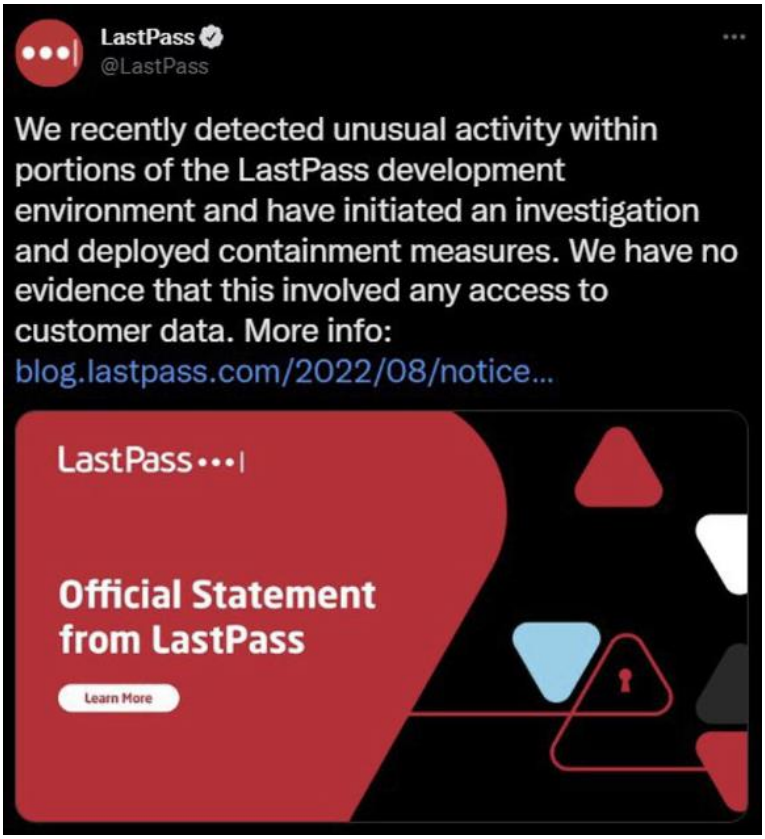
ID de alerta:	DSOC-CERT_2022_08_26_01
Clasificación de alerta:	Noticia
Tipo de Impacto:	ALTO
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	08/26/2022
Es día cero (0 day):	No

Resumen

La brecha parece haber sido de los servidores de desarrollo, facilitada por un compromiso de una cuenta de desarrollador de LastPass y tuvo lugar hace dos semanas. Los respondedores de incidentes han contenido la infracción y LastPass dice que no hay evidencia de más actividad maliciosa. Toubba también confirmó que tampoco se ha encontrado evidencia de que se haya accedido a datos de clientes o bóvedas de contraseñas encriptadas.

¿Su contraseña maestra o su bóveda de contraseñas de LastPass se han visto comprometidas?

LastPass ha dejado claro que, gracias a la arquitectura de "conocimiento cero" implementada, las contraseñas maestras nunca se almacenan. "LastPass nunca puede conocer ni obtener acceso a la contraseña maestra de nuestros clientes", dijo Toubba, "este incidente no comprometió su contraseña maestra". Como tal, LastPass dice que los usuarios no requieren ninguna acción con respecto a sus bóvedas de contraseñas.



No es su primer ataque.

Si bien se debe felicitar a LastPass por la transparencia que se muestra en respuesta a este incidente, no es la primera vez que los usuarios del administrador de contraseñas tienen que lidiar con noticias de una violación. En junio de 2015, la empresa confirmó que los piratas informáticos habían accedido a la red . Entonces, a diferencia de ahora, a los usuarios se les pedía que cambiaran las contraseñas maestras al iniciar sesión.

Inquietudes sobre qué información técnica de LastPass fue robada.

Es una buena noticia que los datos de los clientes no se hayan visto comprometidos en este último incidente, pero el hecho de que el intruso haya accedido al código fuente y a la "información técnica patentada" es preocupante. Sobre todo, porque no hay más detalles sobre lo que se ha robado exactamente.

RECOMENDACIONES

- Si usted es usuario de este software, le recomendamos considerar buscar otra opción en el mercado. Aunque la información de los clientes no fue expuesta el hecho de que sean vulnerados por segunda ocasión es un indicador de alerta para sus usuarios.

- Valide en el inventario de software de su organización si algún usuario tiene instalado este aplicativo y tomar medidas correctivas.

- Permanecer alerta a las noticias y boletines asociados a este ataque.

NOTICIA COMPLETA

https://devel.group/ataque-logra-robar-codigo-fuente-al-aplicativo-lastpass/

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