BOLETÍN DE ALERTA

Boletín Nro.: 2020-25
Fecha de publicación: 31/08/2020
Tema: Vulnerabilidades críticas en Slack Desktop para Windows, Mac y Linux.

Producto afectado:

- Slack Desktop en versiones 4.3 y 4.32 para Windows, Mac y Linux.

Descripción:

Investigadores informan sobre **vulnerabilidades críticas** que afectan a la aplicación **Slack Desktop** para **Windows, Mac y Linux**. Estas vulnerabilidades podrían llevar a la **ejecución remota de código**, si un atacante carga un archivo y lo comparte con otro usuario.

Se ha informado múltiples formas de explotación de dichas vulnerabilidades, por ejemplo con **redireccionamientos en la aplicación**, **redireccionamientos lógicos/abiertos**, e inclusive **inyecciones HTML** y **Javascript**, en ***file.slack.com.***

Un atacante podría cargar un **archivo** con un **payload** de **ejecución remota de código** a un servidor de su propiedad, habilitado para **HTTPS.** Seguidamente, preparar una **publicación de Slack** con la **inyección HTML** y finalmente compartir dicha publicación con un canal o usuario víctima.

Una vez que la víctima haga clic en la publicación compartida, el **código HTML** inyectado redirige la aplicación de escritorio de la víctima al sitio web del atacante, y este sitio responde con un **payload Javascript**, el cual omite el entorno de la aplicación de escritorio **Slack** y **ejecuta comandos arbitrarios** en la computadora de la víctima. Además, dicho payload puede ser modificado fácilmente, para acceder a todas las **conversaciones privadas**, **archivos**, **tokens**, e **información confidencial**, sin necesidad de la ejecución de comandos en la computadora de la víctima.

Además de esto, fue descubierta también una vulnerabilidad de **XSS (Cross-site Scripting)**, la cual se da debido a que los correos electrónicos enviados con "**Send to Slack**" son almacenados sin filtrar, en los servidores de **Slack** en ***file.slack.com***. Esta funcionalidad de **carga de archivos HTML** puede ser utilizada por atacantes para almacenar **payloads** de **ejecución remota de código** sin necesidad de utilizar un hosting propio. Como se trata de un

dominio de confianza, este podría contener **páginas phishing** de inicio de sesión en Slack falsos o cualquier otro **contenido arbitrario** que podría impactar en la seguridad del usuario.

Impacto:

Estas vulnerabilidades podrían permitir a un atacante remoto:

- Acceder a archivos privados, claves privadas, contraseñas, entre otros.
- Acceder a conversaciones privadas y archivos dentro de Slack.
- Inyectar contenido **HTML arbitrario** en la página de confianza ****slack.com***
- Ejecutar código arbitrario en el equipo de la víctima.

Solución y prevención:

Actualizar **Slack Desktop App** a la última versión disponible, en este caso la **versión 4.8.0:**

- **Para Windows**, desde el siguiente **enlace**;
- **Para Linux**, desde el siguiente **enlace**;
- **Para Mac,** desde el siguiente **enlace**.

Información adicional:

- https://slack.engineering/the-app-sandbox/
- https://www.bleepingcomputer.com/news/security/slack-pays-stingy-1-750-reward-for-a-desktop-hijack-vulnerability/
- https://mashable.com/article/slack-fixes-critical-remote-code-execution-vulnerabilitybug-bounty/