Investigadores de seguridad cibernética revelaron una vulnerabilidad crítica sin parchear, que afecta a las tiendas de software libre y de código abierto (FOSS) basados en Pling para la plataforma Linux, y que podría utilizarse para organizar ataques a la cadena de suministro y lograr ejecución remota de código (RCE).

> *«Los mercados de Linux que se basan en la plataforma Pling son vulnerables a un gusano (cross-site-scripting) con potencial para un ataque a la cadena de suministro. La aplicación nativa PlingStore se ve afectada por una vulnerabilidad RCE, que puede activarse desde cualquier sitio web mientras la aplicación se está ejecutando»*, dijo Fabian Bräunlein, cofundador de Positive Security.

Las tiendas de aplicaciones basadas en Pling afectadas por la vulnerabilidad incluyen:

- appimagehub.com
- store.kde.org
- gnome-look.org
- xfce-look.org
- pling.com

PlingStore permite a los usuarios buscar e instalar software, temas, íconos y otros complementos de Linux que pueden no estar disponibles para descargar a través del centro de software de la distribución.

La vulnerabilidad se debe a la forma en que la página de listados de productos de la tienda analiza HTML o los campos multimedia incrustados, lo que permite potencialmente que un atacante inyecte código JavaScript malicioso que podría resultar en la ejecución de código arbitrario.

> *«Este XSS almacenado podría usarse para modificar listados activos, o publicar nuevos listados en la tienda Pling en el contexto de otros usuarios, dando como*

> *resultado un XSS con gusanos»,* dijo Bräunlein.

Más preocupante, esto podría permitir un gusano XSS de ataque a la cadena de suministro en el que un atacante podría explotar una carga útil de JavaScript para cargar versiones de software troyanizadas y modificar los metadatos de la lista de una víctima para incluir y propagar el código de ataque.

Con la aplicación PlingStore actuando como un único escaparate digital para todas las tiendas de aplicaciones antes mencionadas, Positive Security dijo que el exploit XSS se puede activar desde dentro de la aplicación que, al combinarse con una omisión de la zona de pruebas, podría conducir a la ejecución remota de código.

> *«Como la aplicación puede instalar otras aplicaciones, tiene otro mecanismo incorporado para ejecutar código en el nivel del sistema operativo. Resulta que ese mecanismo puede ser aprovechado por cualquier sitio web para ejecutar código nativo arbitrario mientras la aplicación PlingStore está abierta en segundo plano»*, agregó Bräunlein.

En otras palabras, cuando un usuario visita un sitio web malicioso a través del navegador, el XSS se activa dentro de la aplicación Pling mientras se ejecuta en segundo plano. El código JavaScript en el sitio web no solo puede establecer una conexión con el servidor WebSocket local que se utiliza para escuchar los mensajes de la aplicación, sino que también lo usa para enviar mensajes para ejecutar código nativo arbitrario descargando y ejecutando un archivo de paquete .AppImage.

Además, una falla XSS similar descubierta en el mercado de extensiones de GNOME Shell, podría aprovecharse para apuntar a la computadora de la víctima emitiendo comandos maliciosos para la extensión del navegador de integración de Gnome Shell e incluso extensiones publicadas de puerta trasera.

La compañía de seguridad cibernética con sede en Berlín, dijo que las vulnerabilidades se informaron a los respectivos encargados del proyecto el pasado 24 de febrero, y que KDE Project y GNOME Security emitieron parches para los problemas posteriores a la divulgación. Debido a que la vulnerabilidad de RCE asociada con PlingStore aún no se soluciona, se recomienda no ejecutar la aplicación Electron hasta que se haya implementado una solución.

El informe llega a menos de un mes después de que se descubrieron graves vulnerabilidades en distintas extensiones populares de Visual Studio Code, que podrían permitir a los atacantes comprometer máquinas locales, así como construir e implementar sistemas a través del entorno de desarrollo integrado de un desarrollador, allanando el camino para ataques a la cadena de suministro.

> *«Las vulnerabilidades demuestran el riesgo adicional asociado con tales mercados. En este entorno, incluso las vulnerabilidades relativamente pequeñas (por ejemplo, una comprobación de origen faltante) pueden tener consecuencias graves (RCE desde cualquier navegador con la aplicación vulnerable ejecutándose en segundo plano). Los desarrolladores de dichas aplicaciones deben someterse a un alto nivel de escrutinio para garantizar su seguridad»,* dijo Bräunlein.